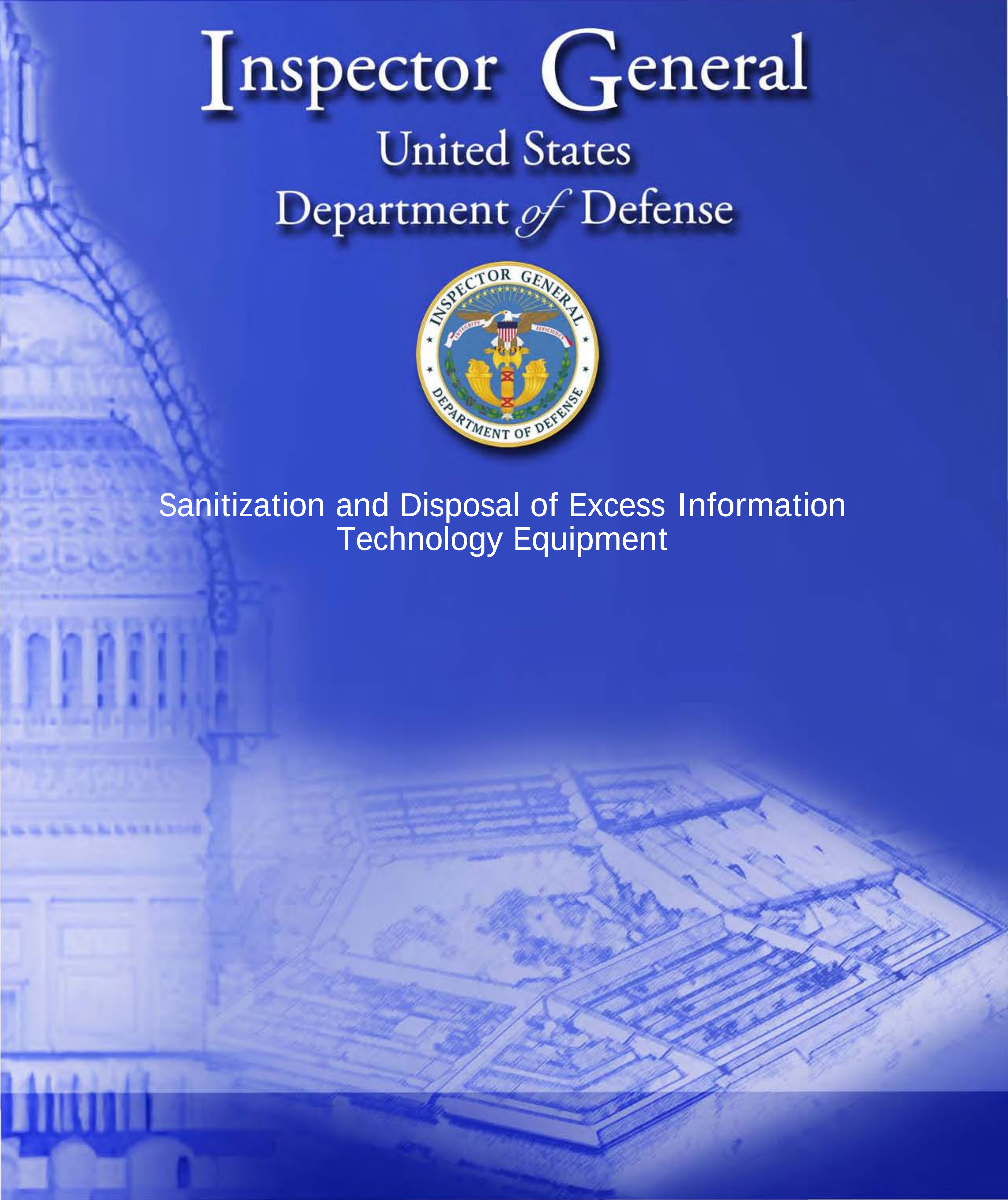
Report No. D-2009-104

September 21, 2009

Inspector General

United States
Department *of* Defense



Sanitization and Disposal of Excess Information Technology Equipment

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **21 SEP 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**
4. TITLE AND SUBTITLE **Sanitization and Disposal of Excess Information Technology Equipment**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,400 Army Navy Drive,Arlington,VA,22202-4704**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**53**	

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms and Abbreviations

AFB	Air Force Base
ASD (NII)/DOD CIO	Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer
DRMS	Defense Reutilization and Marketing Service
IT	Information Technology
NAS	Naval Air Station
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAWCAD	Naval Air Warfare Center Aircraft Division
USACE	U.S. Army Corps of Engineers

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

September 21, 2009

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Sanitization and Disposal of Excess Information Technology Equipment (Report No. D-2009-104)

We are providing this final report for review and comment. We considered comments from the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer; Chief Information Officer, Department of the Navy; Director of Corporate Information, U.S. Army Corps of Engineers; and Commander, U.S. Army Corps of Engineers Louisville District, when preparing the final report. The Commander, 436th Medical Group, Dover Air Force Base, and the Commander, 50th Space Communications Squadron, Schriever Air Force Base, did not respond to the draft report. The complete text of the comments is in the Management Comments section of the report.

DOD Directive 7650.3 requires all recommendations be resolved promptly. The Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer's comments on Recommendation 1 and the Navy Chief Information Officer and Commander, Naval Air Warfare Center Aircraft Division, comments on Recommendations 3, 4, 6.a, 6.b, and 6.c were responsive and require no further comments. The Navy Chief Information Officer and Commander, Naval Air Warfare Center Aircraft Division, comments on Recommendation 6.d and the comments of the Director of Corporate Information, U.S. Army Corps of Engineers, on Recommendation 2 were not responsive because the actions proposed will not fully resolve the issues identified. The comments of the Commander, U.S. Army Corps of Engineers Louisville District, on Recommendation 5 were not responsive because he did not indicate which electronic record-keeping system would be used to track hard drives containing sensitive information that are removed from their computer shells. Therefore, we request comments as indicated in the recommendations table on page ii by October 21, 2009.

Please provide comments that conform to the requirements of DOD Directive 7650.3. If possible, send a .pdf file containing your comments to audros@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8905 (DSN 664-8905).

Paul J Granetto

Paul J. Granetto
Assistant Inspector General
Readiness, Operations, and Support

DISTRIBUTION:

UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND INFORMATION INTEGRATION)/DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE LOGISTICS AGENCY
  DIRECTOR, DEFENSE REUTILIZATION AND MARKETING SERVICE
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
DIRECTOR OF CORPORATE INFORMATION, U.S. ARMY CORPS OF ENGINEERS
COMMANDER, U.S. ARMY CORPS OF ENGINEERS LOUISVILLE DISTRICT
COMMANDER, U.S. ARMY GARRISON WEST POINT
  DIRECTOR OF LOGISTICS, U.S. ARMY GARRISON WEST POINT
COMMANDER, NAVAL AIR SYSTEMS COMMAND
  COMMANDER, NAVAL WARFARE CENTER AIRCRAFT DIVISION
  COMMANDER, NAVAL FACILITIES ENGINEERING COMMAND
COMMANDER, 436TH MEDICAL GROUP, DOVER AIR FORCE BASE
COMMANDER, 50TH NETWORK OPERATIONS GROUP, SCHRIEVER AIR FORCE BASE
  COMMANDER, 50TH SPACE COMMUNICATIONS SQUADRON
COMMANDER, 21ST SPACE WING COMMAND, PETERSON AIR FORCE BASE
COMMANDER, 108TH AIR REFUELING WING, MCGUIRE AIR FORCE BASE
  COMMANDER, 108TH COMMUNICATIONS FLIGHT
  COMMANDER, 108TH LOGISTICS READINESS SQUADRON

Report No. D-2009-104 (Project No. D2008-D000LC-0064.000)   September 21, 2009

Results in Brief: Sanitization and Disposal of Excess Information Technology Equipment

What We Did

We determined whether DOD Components sanitized and disposed of excess unclassified information technology (IT) equipment in accordance with Federal and DOD requirements. We also determined whether the Defense Reutilization and Marketing Service (DRMS) disposed of excess IT equipment in accordance with security requirements; and whether the Army, Navy, and Air Force properly safeguarded sensitive information on excess unclassified IT equipment. We visited 6 DOD Components, 9 DRMS processing centers, and 2 contractors and selected a non-statistical sample 543 of 4,105 pieces of excess unclassified IT equipment.

What We Found

DOD Components' internal controls were not adequate. Specifically, DOD Components did not properly sanitize, document, or fully account for excess unclassified IT equipment before releasing the equipment to other organizations. Furthermore, DRMS processing centers processed excess unclassified IT equipment for disposal or redistribution without proof that equipment had been properly sanitized.

These instances of nonperformance occurred because DOD Components did not follow policies, adequately train personnel, or develop and implement site-specific procedures to ensure excess unclassified equipment was sanitized and disposed of properly. Additionally, DOD guidance issued by the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer and the Navy Chief Information Officer was out of date and did not cover sanitizing and disposing of new types of information storage devices.

As a result, four DOD Components could not ensure personally identifiable information or other sensitive DOD information was protected from unauthorized release, and one DOD Component could not account for an excess unclassified computer.

What We Recommend

We recommended that:

- the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer and the Deputy Chief of Naval Operations for Communications Networks update current sanitization and disposal policies to ensure they address current technology issues;
- the Department of the Navy Chief Information Officer establish and implement a clear, detailed policy for sanitizing and disposing of excess IT equipment including electronic storage devices; and
- DOD Components sanitize and account for excess unclassified IT equipment in accordance with applicable laws and regulations.

Management Comments and Our Responses

The Commander, 436th Medical Group, and the Commander, 50th Space Communications Squadron, did not provide comments on the draft report issued on June 25, 2009. We request comments from them on the final report by October 21, 2009. Management comments we received were partially responsive. We request additional comments from the responding organizations as indicated in the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer		1
Director of Corporate Information, U.S. Army Corps of Engineers	2	
Department of the Navy Chief Information Officer	6.d	3
Deputy Chief of Naval Operations for Communications Networks		4
Commander, U.S. Army Corps of Engineers Louisville District	5.a and 5.b	
Commander, Naval Air Warfare Center Aircraft Division	6.d	6.a; 6.b; and 6.c
Commander, 436th Medical Group, Dover Air Force Base	7.a and 7.b	
Commander, 50th Space Communications Squadron, Schriever Air Force Base	7.a and 7.b	

Please provide comments by October 21, 2009.

Table of Contents

Results in Brief i

Introduction 1

Objectives 1
Background 1
Review of Internal Controls 3

Finding. Protecting Sensitive Information and Accounting for Excess Information Technology Equipment 4

Recommendations, Management Comments, and Our Response 13

Appendices

A. Scope and Methodology 19
Prior Coverage 21
B. Label Certifying Hard Drive Disposition 22
C. Immediate Action Memoranda to DOD Components 23

Management Comments

Assistant Secretary of Defense (Networks and Information Integration)/ DOD Chief Information Officer 38
Department of the Navy Chief Information Officer 39
U.S. Army Corps of Engineers Directorate of Corporate Information 43
U.S. Army Corps of Engineers Louisville District 44

Introduction

Objectives

Our audit objective was to determine whether DOD Components sanitized and disposed of excess unclassified information technology (IT) equipment[1] in accordance with Federal and DOD regulations. We also determined whether the Army, Navy, and Air Force properly safeguarded sensitive information on excess unclassified IT equipment by sanitizing and accounting for the equipment before forwarding it to Defense Reutilization and Marketing Service (DRMS) and whether the DRMS disposed of excess IT equipment in accordance with DOD requirements. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objective.

Background

DOD Guidance

The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence[2] Memorandum, "Disposition of Unclassified DOD Computer Hard Drives" (Disposition Memorandum), June 4, 2001, states that no information is to remain on unclassified IT equipment hard drives that are reused or permanently removed from DOD custody. The Disposition Memorandum outlines three acceptable methods for hard drive sanitization:

- Overwriting the hard drive by using software that replaces previously stored hard drive data with meaningless information. Only this method enables a hard drive to be redistributed for reuse.

- Degaussing a hard drive by demagnetizing it using a National Security Agency approved degausser. Properly applied, degaussing renders data on the hard drive unreadable. After degaussing, hard drives can seldom be used.

- Physically destroying a hard drive to ensure it is not usable in a computer and that no data can be recovered or read. Sufficient force is applied to the top of the hard drive unit to damage the disk surface. In addition, connectors that interface with the computer must be mangled, bent, or damaged to the point that the hard drive cannot be reconnected without significant rework. Before a hard drive is physically destroyed, it should be overwritten or degaussed. This method results in the hard drive being unusable.

[1] IT equipment that processed or contained unclassified information.

[2] The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence used to fulfill Chief Information Officer duties; those duties now belong to the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer.

In addition, the Disposition Memorandum requires DOD Components to complete a disposition label certifying that sanitization has been performed. The completed disposition label must be attached to the hard drive or the computer housing the hard drive. The disposition label details basic information about the DOD Component, computer, and hard drive; the method and software used to sanitize the hard drive, if applicable; the method for destroying the hard drive, if applicable; and the signature and contact information for the DOD Component personnel that performed the sanitization.

DOD Components send their excess IT equipment to DRMS processing centers. DRMS processing centers make excess IT equipment available to another DOD Component, another Federal agency, or a school or other nonprofit organization; sell it to the public; or destroy it.

DOD Components are required to sanitize excess or surplus unclassified IT equipment in accordance with the Disposition Memorandum before sending it to a DRMS processing center. DRMS is responsible for training DOD Components on turn-in procedures, including inspecting and classifying property, verifying identity and quantity on disposal documentation, and maintaining property accountability for and control of excess equipment.

Based on the DOD Directive 8100.01, "Global Information Grid Overarching Policy," November 21, 2003, definition of IT equipment,[3] we identified the following as IT equipment: computers (desktops and laptops), external/auxiliary hard drives, printers, scanners, cell phones, personal digital assistants, removable storage devices (such as thumb drives, moving picture experts group audio layer III [mp3] players, diskettes, compact discs, digital video discs, and subscriber identity module cards). During FYs 2007 and 2008, DOD disposed of 340,349 pieces of useable IT equipment and 57,485,000 pounds of scrap IT equipment.

DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006, requires that an electronic property receipt record be maintained throughout the property's life cycle regardless of its status (acquisition, in-service, unserviceable, obsolete, excess, surplus) or physical location. To account for the IT assets, this Instruction also requires that excess unclassified IT equipment with a unit acquisition cost of $5,000 or more, or equipment that is considered to be sensitive, be accounted for in an electronic record-keeping system until the activity receiving the equipment confirms its receipt in writing.

Industry Sanitization Guidelines

The National Institute of Standards and Technology is responsible for developing standards and guidelines for providing adequate information security for all Federal

[3] DOD Directive 8100.01 defines IT equipment as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by a DOD Component.

agency operations and assets. National Institute of Standards and Technology Special Publication 800-88, “Guidelines for Media Sanitization,” September 2006, outlines specifications for the:

- sanitization and disposal of information storage devices based on ownership;
- overwriting, degaussing, and destruction of excess information storage devices; and
- completion of sanitization, disposition, and accountability documents.

National Institute of Standards and Technology Special Publication 800-88 requires organizations to develop and use local policies and procedures in conjunction with this publication to decide the method of sanitization and disposition of information storage devices.

Review of Internal Controls

At the sites visited, we identified internal control weaknesses as defined by DOD Instruction 5010.40, “Managers’ Internal Control (MIC) Program Procedures,” January 4, 2006. DOD Components and DRMS processing centers did not follow relevant DOD policies, adequately train personnel, or develop and implement site-specific procedures to ensure excess unclassified IT equipment was properly sanitized and accounted for. In addition, DOD and Navy policies governing the sanitization of excess IT equipment were outdated. Implementing Recommendations 1 through 7 will improve DOD sanitization and disposal processes. We will provide a copy of this report to the senior officials responsible for internal controls for the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer (ASD[NII])/DOD CIO) and the Army, Navy, and Air Force.

Finding. Protecting Sensitive Information and Accounting for Excess Information Technology Equipment

DOD Components did not properly sanitize, document, or fully account for excess unclassified IT equipment before it was released to other Federal, DOD, or non-Federal organizations. In addition, DRMS processing centers processed excess unclassified IT equipment without documentation that the equipment was properly sanitized. DOD Components and DRMS processing centers fell short because they did not follow DOD policies, adequately train personnel, or develop and implement site-specific procedures to ensure excess unclassified IT equipment was properly accounted for and sanitized. Furthermore, DOD and Navy policies governing the sanitization of excess IT equipment are outdated. As a result, four DOD Components could not ensure that personally identifiable information or other sensitive DOD information was protected from unauthorized release, and one DOD Component could not account for an excess unclassified computer.

Processing Excess Unclassified IT Equipment

DOD Components are required to sanitize excess IT equipment before disposal to protect sensitive DOD information, as well as other sensitive information such as personally identifiable information, from public disclosure. Public disclosure of this information can cause harm to DOD and its operations and potentially to individuals whose personal information has been compromised. Therefore, this process is required to be adequately documented to ensure required procedures have been followed. Finally, DOD Components are also required to properly maintain and account for IT equipment throughout its life cycle.

Sanitizing Excess Unclassified IT Equipment

DOD Components did not properly sanitize IT equipment before processing it for reuse, transfer, donation, or destruction in accordance with the Disposition Memorandum. The Disposition Memorandum requires that no information is to remain on hard drives of unclassified IT equipment that are reused or permanently removed from DOD custody. At 4 locations we identified 10 pieces of excess unclassified IT equipment that contained readable information on hard drives. Specifically, the following pieces of excess unclassified IT equipment contained readable information.

- An electrocardiogram machine waiting to be shipped from the 436th Medical Group at Dover Air Force Base (AFB), Delaware, to another Air Force component contained the full names and Social Security numbers of three patients. Officials told us that the electrocardiogram machine contained this information because the 436th Medical Group personnel were unaware that some medical equipment, such as electrocardiogram machines, contained hard drives.

The 436th Medical Group officials said they had not been properly trained to sanitize all types of excess unclassified IT equipment.

- Five hard drives waiting to be shipped from the Naval Air Warfare Center Aircraft Division (NAWCAD), Naval Air Station (NAS) Patuxent River, Maryland, to a DRMS processing center contained readable information. One computer contained information such as phone numbers, e-mail addresses, instant messaging traffic, pictures, and various system log files. These hard drives contained information because the Naval Air Systems Command (NAVAIR) and NAWCAD had not adequately trained personnel responsible for sanitizing equipment or developed site-specific policies that clearly defined sanitization and disposal roles and responsibilities. For example, NAWCAD lab personnel had not received formal training on degaussing equipment and, in one instance, used an audio-video degausser to degauss hard drives.

- Three hard drives waiting to be redistributed from the 50th Space Communications Squadron, Schriever AFB, Colorado, to another Schriever AFB command contained personal user folders or default operating system information. The information remained on the equipment because the 50th Space Communications Squadron had not established and implemented a process ensuring that excess unclassified IT equipment containing more than one hard drive was properly sanitized. Two of the three hard drives that were not properly sanitized were pulled from computers that housed more than one hard drive, and the equipment custodian did not physically verify whether these computers contained more than one hard drive. No explanation was available as to why the third hard drive had not been properly sanitized.

- A hard drive sent from the U.S. Army Garrison West Point, New York, to a DRMS processing center contained bytes of random characters. Officials told us that this occurred because the U.S. Army Garrison West Point did not properly train personnel. In addition, U.S. Army Garrison West Point did not follow proper procedures by performing the required verification of sanitized excess unclassified IT equipment before sending equipment to a DRMS processing center.

During our site visit in June 2008, the U.S. Army Corps of Engineers (USACE) Louisville District, Louisville, Kentucky, was properly sanitizing excess hard drives. However, in August 2008 the Director of Corporate Information instituted a new process for the sanitization and disposal of USACE excess hard drives whereby a contractor physically destroys them. The new process is outlined in the draft Army Corps of Engineers IT Standard Operating Procedure, "Process for Hard Drive Destruction," August 6, 2008. The Army Corps of Engineers IT Standard Operating Procedure requires the physical destruction of hard drives to be conducted in accordance with Army Regulation 25-2, "Information Assurance," October 24, 2007. Yet whereas Army Regulation 25-2 requires all excess unclassified Army hard drives to be overwritten or degaussed before leaving DOD custody, the Army Corps of Engineers IT Standard

Operating Procedure does not require hard drives to be overwritten or degaussed before shipping to the contractor. As a result of changing the process, USACE cannot ensure DOD information is properly protected from unauthorized release.

As a result of these weaknesses, five DOD Components sent or were preparing to send excess IT equipment containing DOD information (including personally identifiable information) to other Federal, DOD, or non-Federal organizations.

Documenting Sanitization of Excess Unclassified IT Equipment

Five DOD Components did not properly complete documentation for excess unclassified IT equipment submitted to DRMS processing centers. The Disposition Memorandum states that once sanitization has been carried out, a signed disposition label[4] must be attached to the hard drive or the computer housing the hard drive. Disposition labels verify that the equipment was properly sanitized. The disposal turn-in documents provide DRMS processing centers with key information needed to process excess equipment. During fieldwork we identified the following examples of the lack of supporting documentation.

- USACE Louisville District did not accurately complete disposition labels for 4 of the 10 computers sampled. Two disposition labels were missing the sanitization date, one disposition label was missing the make and model, and the fourth disposition label had no signature date. The disposition labels were not properly completed because USACE Louisville District did not adequately train responsible personnel to properly complete disposition labels.

- The U.S. Army Garrison West Point did not properly prepare disposition labels for two of four excess unclassified hard drives. The hard drives did not have a disposition label or did not have a properly prepared disposition label. One of these computers contained information on its hard drive. Officials said the disposition labels were not attached or were improperly prepared because the U.S. Army Garrison West Point did not adequately train the responsible personnel to attach or complete disposition labels.

- Two NAVAIR data centers and two labs located at NAS Patuxent River did not complete disposition labels for excess unclassified IT equipment. This occurred because personnel were not aware of the Disposition Memorandum requirements. In addition, three NAWCAD computers were turned into the Naval Facilities Engineering Command (NAVFAC) Property Disposal Office without disposal turn-in documents. Furthermore, for one sampled computer, NAWCAD personnel generated and submitted a duplicate disposal turn-in document number[5]

[4] See Appendix B for a more detailed description of a hard drive disposition label showing the types of information DOD Components frequently omitted.

[5] The disposal turn-in document number is a distinct 14-digit number that consists of the DOD activity's six-digit DOD activity address code, four-digit Julian date, and four-digit serial number.

to a DRMS processing center. The NAVFAC Property Disposal Office personnel did not know which NAS Patuxent River activity had turned in three computers without supporting documentation. Barcodes indicated that the computers belonged to NAWCAD, but that was insufficient information to determine which NAWCAD division owned the computers. Furthermore, NAWCAD personnel created duplicate disposal turn-in document numbers because personnel used different methods that did not interface to generate disposal turn-in document numbers.

- The 108th Air Refueling Wing at McGuire AFB, New Jersey, did not attach or fully complete disposition labels for 92 pieces of excess unclassified IT equipment. Wing personnel did not attach disposition labels to 51 hard drives and did not indicate the method of sanitization for 41 computer shells. They also did not attach or complete disposition labels as required by the Disposition Memorandum and Air Force System Security Instruction 5020, "Communications and Information Remanence Security," April 17, 2003.

- The 50th Space Communication Squadron at Schriever AFB did not attach disposition labels to six computers because personnel did not follow the Disposition Memorandum or Air Force Instruction 5020, which require that a disposition label be attached to the hard drive or the computer housing the hard drive. We were told that the 50th Space Communications Squadron personnel attach disposition labels only to computers being sent to DRMS processing centers.

In addition, DRMS processing centers processed 108 out of 148 pieces of excess unclassified IT equipment without documentation that the equipment had been properly sanitized. Nine DRMS processing centers processed 41 pieces of equipment that did not include disposition labels, 64 pieces of equipment that had incomplete disposition labels,[6] and 3 pieces of equipment that had inaccurate disposition labels.[7] Appendix B shows an example of the disposition label highlighting the types of missing information. Officials said that DRMS processed excess unclassified IT equipment without supporting documentation because DRMS had experienced significant turnover in personnel and had not trained new staff.

Since five DOD Components did not properly complete supporting documentation and nine DRMS processing centers processed excess unclassified IT equipment without proper documentation, DOD was unable to ensure that information contained on excess unclassified IT equipment was properly protected from unauthorized release.

[6] Incomplete disposition labels are labels that did not have the date and signature from the DOD Component verifying that the hard drive was sanitized or did not state the method of sanitization.

[7] Inaccurate disposition labels are labels that did not accurately reflect the equipment status (for example, a disposition label stating that the hard drive was removed, attached to a computer in which the hard drive was present).

Accounting for Excess Unclassified IT Equipment

DOD Components did not account for excess unclassified hard drives after they were removed from computer shells, nor did they account for other pieces of excess unclassified IT equipment throughout their life cycle. DOD Instruction 5000.64 requires that excess unclassified IT equipment having a unit acquisition cost of $5,000 or more and assets that are sensitive be accounted for in an electronic record-keeping system until the activity receiving the equipment confirms receipt of equipment in writing. This requirement ensures that the information contained on the equipment is protected and the equipment itself is accounted for throughout its life cycle.

At 5 of the 15 locations visited, DOD personnel did not account for hard drives after they were removed from computer shells. At 2 of the 15 locations, personnel did not account for other pieces of excess IT equipment throughout their life cycle. Following are examples of the accountability issues identified.

- USACE Louisville District did not account for 11 excess unclassified hard drives after they were removed from their computer shells. USACE Louisville District standard operating procedure did not include procedures to electronically account for physically removed hard drives. For example, USACE did not have an electronic log to document hard drives that were stockpiled and unable to be properly sanitized.

- NAVAIR labs and data centers at NAS Patuxent River did not electronically account for excess unclassified hard drives that had been removed from the computer shells. Personnel were unaware that they needed to account for hard drives removed from their computer shells. In addition, the NAWCAD Property Management Team removed the equipment from the Navy Enterprise Resource Planning system too early. The team should have waited to remove the equipment from the system until they received documentation from DRMS stating that the equipment had been received and processed. Instead, the NAWCAD Property Management Team removed the equipment from the system when they received a receipt from the NAVFAC Property Disposal Office.

- The 436th Medical Group at Dover AFB did not electronically account for 105 hard drives removed from their computer shells because personnel were unaware that removed hard drives in the process of being degaussed needed to be accounted for electronically.

- The 108th Air Refueling Wing at McGuire AFB did not account for 92 pieces of excess unclassified IT equipment throughout their entire life cycle. Personnel removed IT equipment from the electronic record-keeping system too early. The 92 pieces of excess unclassified IT equipment were removed from the electronic record-keeping system when they were turned into the Communications Flight Unit for sanitization and disposal instead of when DRMS received and processed them.

- The 50th Space Communications Squadron at Schriever AFB did not electronically account for hard drives removed from their computer shells because personnel considered hard drives to be accounted for as part of the original computer shell.

DOD did not properly account for at least 208 pieces of excess unclassified IT equipment in an electronic record-keeping system because DOD Components did not consider physically removed hard drives accountable assets. Therefore, personnel did not follow established criteria. As a result, DOD cannot ensure that excess unclassified IT equipment is accounted for or properly protected from unauthorized release. It is imperative that DOD Components account for excess unclassified IT equipment throughout its life cycle to protect information on the equipment. For the same reason, it is critical to account for hard drives removed from their computer shells.

DOD and Navy Sanitization Policies

DOD Components are required to ensure the timely issuance and updating of policies governing DOD operations, functions, and programs. Specifically, Components are required to review existing policies periodically to determine whether the policies should be updated, incorporated in or converted to a DOD issuance, reissued, or canceled. If DOD Component personnel fail to conduct the periodic reviews and updates, critical policies may not provide the specific guidance needed to carry out DOD functions effectively.

DOD Policy

The ASD(NII)/DOD CIO has not updated the Disposition Memorandum since it was issued in June 2001. The Disposition Memorandum's policies and procedures were intended to ensure that all hard drives contained in excess unclassified computers were properly sanitized before being disposed of outside DOD. However, the Disposition Memorandum does not address other types of DOD information storage devices in use at the time—such as printers and fax machines—nor has it been updated to include new information storage devices, such as thumb drives, compact discs, digital video devices, and digital data or voice recorders, which can also contain sensitive DOD information. The failure to include all current types of information storage devices in the Disposition Memorandum creates vulnerability that these devices will not be properly sanitized of all sensitive information before disposal.

Furthermore, DOD Instruction 5025.01, "DOD Directive Program," October 28, 2007, requires that a DOD Directive-Type Memorandum be incorporated in existing policy, converted to a new policy, reissued, or canceled within 180 days of the issuance of the Instruction. The ASD(NII)/DOD CIO has not followed the Instruction.

An ASD (NII)/DOD CIO Senior Policy Analyst stated he had not updated the Disposition Memorandum because of the competing priorities of national security and scarce resources.

Navy Policy

The Department of the Navy has not updated Navy-specific criteria for the sanitization and disposal of excess IT equipment to fully implement the Disposition Memorandum. Nor has the Navy updated its instructions to include newer information storage devices such as thumb drives and digital video devices. The Deputy Chief of Naval Operations for Communications Networks has not updated Navy Information Assurance Publication 5239-26 since it was issued in May 2000.[8] The Navy Publication provides instructions to Navy Components on:

- sanitization of electronic storage media for later reuse,
- methods for destruction of electronic storage media, and
- removal of external markings from electronic storage media.

The Disposition Memorandum outlines policies and procedures to ensure that hard drives in excess unclassified computers are properly sanitized before being disposed of outside of DOD. The Navy Publication includes the three sanitization methods outlined in the Disposition Memorandum, but does not require the completion and attachment of the disposition label validating that the hard drive was sanitized. Also, the Navy Publication does not require the verification of overwriting, the method used to sanitize at least 20 percent of the Navy's excess hard drives. Therefore, Navy Components were not required to include completed disposition labels or validate that sanitization had actually occurred before releasing the excess IT equipment for disposal outside DOD.

According to an official from the Office of the Deputy Chief of Naval Operations for Communications Networks, the Navy publication had not been updated because the Navy had competing priorities and scarce resources.

The DOD Disposition Memorandum and Navy Publication 5239-26 are out-of-date and do not contain requirements needed to address all types of information storage devices and to ensure these devices are sanitized and disposed of correctly to protect sensitive data. The lack of specific, up-to-date guidance is contributing to DOD Components' not sanitizing and disposing of all types of IT equipment properly, including information storage devices.

Corrective Actions

We issued memoranda to Commander, 436th Medical Group, Dover AFB; Commander, U.S. Army Garrison West Point; Director of Information Management, U.S. Army Garrison West Point; Commander, 108th Air Refueling Wing, McGuire AFB; Commander, 108th Communications Flight; Commander, 108th Logistics Readiness Squadron; Commander, 50th Network Operations Group; Commander, 50th Space

[8] Army Regulation 25-1, "Army Knowledge Management and Information Technology," July 15, 2005, and Air Force System Security Instruction 5020, "Communications and Information Remanence Security," April 17, 2003, both incorporate the requirements of the Disposition Memorandum. In addition, both instructions include guidance on the sanitization of new types of information storage devices.

Communications Squadron, Schriever AFB; Commander, Naval Air Systems Command Patuxent River; Commander, Naval Air Warfare Center Aircraft Division, and Deputy Public Works Officer, Naval Facilities Engineering Command. See Appendix C for the full text of the five memoranda. The memoranda provided feedback on areas of concern that needed management's immediate attention. DOD Components have taken preliminary steps to correct weaknesses identified; however, additional work is needed. The additional work needed is addressed in our recommendations.

Actions to Improve Information Security

As a result of the audit, the Components recognized the need to adequately sanitize IT equipment, train personnel, and establish written policies and procedures. Since our site visits, officials have taken the following steps to strengthen the sanitization and disposal process.

- As of November 2008, the USACE Louisville District required the completion and attachment of a property control receipt and a disposition label to all excess computers and hard drives removed from their computer shells.

- The U.S. Army Garrison West Point has established policy that outlines procedures for proper sanitization of excess unclassified IT equipment. According to the Garrison Commander, the policy will identify organizational responsibilities and training requirements. The Directorate of Information Management will provide the training, and has scheduled training on the sanitization and disposal of information storage devices for the third quarter of FY 2009. Finally, the Director of the Internal Review and Audit Compliance Office at West Point plans to conduct a compliance review during the third quarter of FY 2009.

- According to the Commander, Naval Air Systems Command, NAWCAD intends to coordinate with the NAVAIR Chief Information Officer to develop appropriate processes and procedures relating to sanitization and disposal of excess IT equipment and will use only one system to generate disposal turn-in documents. However, they do not believe that the ETID system will be the one. In addition, the NAVFAC Deputy Public Works Officer at NAS Patuxent River has started updating written policy to clarify the process for sanitizing and disposing of excess IT equipment.

- The Commander, 436th Medical Group, Dover AFB, implemented a process in July 2008 to check medical equipment for embedded hard drives and remove personally identifiable information before sending the equipment to DRMS processing centers. All biomedical equipment repair technicians and medical information systems technicians at the 436th Medical Group have been trained on the new procedures for removing and degaussing equipment and using authorized overwriting software to clean hard drives. In addition, the 436th Medical Group asked the Air Force Medical Logistics Office to include the new procedures in the Air Force Instruction governing medical equipment maintenance and repair.

- The 108th Communications Flight, McGuire AFB is now completing and attaching disposition labels to the outside of excess computers and hard drives removed from their computer shells.

- The Commander, 50th Network Operations Group, and the 50th Communications Squadron, Schriever AFB, are implementing requirements to verify the number of hard drives in an IT unit when the equipment is turned in. The two units are also developing sanitization training, purchasing degaussing equipment, and updating current procedures to incorporate the requirements in Air Force System Security Instruction 8580. According to the lead equipment custodial officer, since June 2008, personnel from the 50th Network Group and the 50th Communications Squadron have been completing and attaching disposition labels to IT equipment being sanitized and reused within the 50th Network Operation Group and the 50th Communications Squadron.

- According to DRMS personnel, DRMS is revising the Compliance Assessment Program to address the proper process for receiving computer hard drives. DRMS is developing a new training course called "Guidance for Computers, Hard Drives, Electronic Test Equipment, Cell Phones, Fax Machines, Printers, and Land Mobile Radios." Furthermore, management at the DRMS Mechanicsburg processing center immediately held a stand-down with all receiving employees to provide remedial refresher training reiterating the instructions for the proper processing of computers.

These DOD Components have taken corrective action to address some of the internal control weaknesses identified during the audit; therefore, we are not making recommendations related to the corrective actions taken.

Actions to Improve Property Accountability

As a result of our audit, the Commander, 108th Communications Flight, recognized the need to properly account for excess unclassified IT equipment. The 108th Communications Flight, McGuire AFB, created an additional equipment custodian account in the Information Technology Automated Management System to maintain 100-percent accountability for customer turned-in IT equipment that is considered excess. In addition, the 108th Communications Flight unit developed an Excel spreadsheet application to maintain 100-percent accountability for hard drives that are removed from computers or laptops. Therefore, we are not making a recommendation to the Commander, 108th Communications Flight, on these issues.

Actions to Improve Physical Protection of Excess Hard Drives

During the audit, we informed the Commander, 108th Communications Flight, of the lack of sufficient physical protection for excess hard drives removed from computer shells. Although the Commander, 108th Communication Flight, felt physical security measures were sufficient, he agreed to improve the physical protection of excess hard drives. Since our site visit, the 108th Communications Flight, purchased locks for the storage containers that housed the excess hard drives, and personnel label the storage containers to indicate which hard drives are awaiting sanitization and which ones are sanitized. Therefore, we are not making a recommendation to the Commander, 108th Communications Flight, on this issue.

Conclusion

The six DOD Components visited or contacted did not properly sanitize, document, or fully account for excess unclassified IT equipment before it was released to other Federal, DOD, or non-Federal organizations. Also, eight of the nine DRMS processing centers visited processed excess unclassified IT equipment without documentation that the equipment was properly sanitized. Action has been taken to correct some of the problems identified during the audit. Implementing the following recommendations will further improve DOD sanitization and disposal processes for excess unclassified IT equipment and ensure that all problems identified are corrected.

Recommendations, Management Comments, and Our Response

1. We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer, in accordance with DOD Instruction 5025.01, "DOD Directive Program," October 28, 2007, update the memorandum, "Disposition of Unclassified DOD Computer Hard Drives," June 4, 2001 (Disposition Memorandum), to incorporate guidelines for sanitizing and disposing of all types of information technology equipment, including other information storage devices. When updating the Disposition Memorandum, the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer should consider the requirements outlined in National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," September 2006.

Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer Comments

The Principal Director to the Deputy Assistant Secretary of Defense for Cyber, Information, and Identity Assurance, responding for the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer, agreed. He stated the Disposition Memorandum will be updated and incorporated in DOD Directive 8500.01E, "Information Assurance," October 24, 2002, certified current as of April 23, 2007, and DOD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, by the end of 2009.

Our Response

The comments of the Principal Director were responsive. No additional comments are required.

2. We recommend that the Director of Corporate Information, U.S. Army Corps of Engineers, reinstitute overwriting or degaussing of hard drives before shipping the hard drives to the contractor.

U.S. Army Corps of Engineers Comments

The Director of Corporate Information, USACE, agreed with comments on the disposal procedures. The Director stated that the procedures for shipping hard drives had been suspended pending the audit finding but have since been revised. The Director stated that the excess hard drives are being shipped for destruction to a facility approved by the U.S. General Services Administration and are not being released for reuse. Therefore, he asserted that neither overwriting nor degaussing the hard drives is required under DOD regulations. In addition, the Director stated that controls and oversight were in place to protect the information contained on these unclassified hard drives during transport. According to the Director, because of personnel and funding constraints, USACE has chosen to destroy the hard drives at a facility rather than onsite. Finally, the Director stated that the revised procedures comply with Army Regulations, protect the information contained on the hard drives, and are cost-effective. These revised procedures were to be in place by August 30, 2009.

Our Response

The comments of the Director of Corporate Information, USACE, were partially responsive. We agree that USACE had suspended shipping hard drives to destruction facilities. Also, we commend the USACE for the additional controls put in place when transporting the hard drives for destruction at an approved facility. However, if USACE does not, at a minimum, overwrite the hard drives that are to be removed from service before transporting them for destruction, the USACE procedures do not meet the requirements outlined in Section 3.1.1 of the Disposition Memorandum. Section 3.1.1 requires hard drives to be overwritten before reuse or removal from service. If the hard drives are to be removed from service, the hard drives are also required to be degaussed or destroyed. Sensitive data, such as personally identifiable information, could be compromised during the storage and transportation of the hard drives—especially since the hard drives are leaving DOD custody. If Section 3.1.1 is followed and the hard drives are overwritten by the user as required, there should be no readable data on the hard drives to be compromised. Therefore, we do not believe that the USACE procedures fully meet the requirements of Section 3.1.1. We request that the Director of Corporate Information, USACE, reconsider his position on the recommendation and provide additional comments in response to the final report.

3. We recommend that the Navy Chief Information Officer establish and implement guidelines for sanitizing and disposing of all types of information technology equipment including other information storage devices in accordance with current and future sanitization and disposal policy issued by the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer. When establishing and implementing guidelines, the Navy Chief Information

Officer should consider the requirements outlined in National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," September 2006.

Department of the Navy Comments

The Navy Chief Information Officer agreed. The Acting Deputy Chief Information Officer stated that the Chief Information Officer will coordinate and establish the recommended policy within the Department, including the Navy, Marine Corps, and the Chief of Naval Operations Special Assistant for Security, with an estimated completion date of December 30, 2009.

Our Response

The comments of the Acting Deputy Chief Information Officer were responsive, and no additional comments are required.

4. We recommend that the Deputy Chief of Naval Operations for Communications Networks update Navy Information Assurance Publication 5239-26, "Remanence Security Guidebook," May 2000, to comply with the current version of the Disposition Memorandum, "Disposition of DOD Computer Hard Drives," June 4, 2001, and any updates coming out of Recommendation 1.

Department of the Navy Comments

The Navy Chief Information Officer and the Deputy Chief of Naval Operations for Communications Networks agreed. The Acting Deputy Chief Information Officer stated that the Deputy Chief of Naval Operations for Communications Networks will work with the Acting Deputy Chief Information Officer to release guidance that addresses the weaknesses identified in this report. The estimated release date for the new guidance is December 30, 2009. Furthermore, the Deputy Chief of Naval Operations for Communications Networks will coordinate and update Navy Information Assurance Publication 5239-26, "Remanence Security Guidebook," May 2000, to fully implement the Disposition Memorandum, "Disposition of DOD Computer Hard Drives," June 4, 2001; include additional types of electronic storage devices; and consider National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," September 2006. She estimated the update of Navy Information Assurance Publication 5239-26 will be completed by January 29, 2010.

Our Response

The comments of the Acting Deputy Chief Information Officer and the Deputy Chief of Naval Operations for Communications Networks were responsive, and no additional comments are required.

5. We recommend that the Commander of the U.S. Army Corps of Engineers Louisville District:

a. Account for all hard drives removed from their computer shells.

b. Account for hard drives removed from their computer shells that contain sensitive information in an electronic record-keeping system as required by DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006.

U.S. Army Corps of Engineers Louisville District Comments

The Commander, USACE Louisville District, agreed. He stated that the Louisville District has implemented corrective actions to account for the hard drives of any computers that are not a part of the Army Corps of Engineers IT refresher program. Specifically, the USACE Louisville District will attach a disposition label and property control receipt to all excess computers and hard drives. Further, if guidance for the Army Corps of Engineers IT refresher program is not provided by headquarters, the USACE Louisville District will store the equipment until guidance is provided. Finally, the USACE Louisville District has implemented an electronic record-keeping system to track equipment that contains sensitive information in accordance with DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006.

Our Response

The comments of the Commander, USACE Louisville District, are generally responsive. We agree with the corrective actions that are planned. However, the Commander did not provide estimated completion dates for the corrective actions. Also, for Recommendation 5.b, the Commander did not indicate which electronic record-keeping system would be used to track hard drives containing sensitive information that are removed from their computer shells. The only additional comments needed are the estimated dates of completion for these actions and the electronic record-keeping system that will be used to track the hard drives.

6. We recommend that the Commander of the Naval Air Warfare Center Aircraft Division:

a. Require all personnel responsible for sanitization and disposal to comply with the memorandum, "Disposition of Unclassified DOD Computer Hard Drives," June 4, 2001, and any future updates.

b. Account for all hard drives removed from their computer shells.

c. Account for hard drives removed from their computer shells that contain sensitive information in an electronic record-keeping system as required by DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006.

d. Remove excess information technology equipment from the Navy Enterprise Resource Planning System only after obtaining an official receipt from the Defense Reutilization and Marketing Service processing center, as required by

DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006.

Department of the Navy Comments

The Navy Chief Information Officer and the Commander of the Naval Air Warfare Center Aircraft Division agreed with Recommendation 6.a. Specifically, the Commander stated that personnel responsible for the disposal of hard drives would be trained to ensure compliance with the Disposition Memorandum, "Disposition of DOD Computer Hard Drives," June 4, 2001. The estimated completion date for the training is November 30, 2009.

The Navy Chief Information Officer and the Commander of the Naval Air Warfare Center Aircraft Division agreed with Recommendations 6.b and 6.c. The Commander stated that the division will perform an evaluation of existing electronic systems or develop a new system to electronically account for all hard drives removed from their computer shells. In addition, he stated the division will no longer use the National Security Agency to destroy hard drives, but will coordinate disposal of excess hard drives with the Defense Reutilization Marketing Service. The Commander estimated that these actions will be completed by December 31, 2009.

The Navy Chief Information Officer and the Commander of the Naval Air Warfare Center Aircraft Division agreed with Recommendation 6.d. According to the Commander, the Property Management Team will remove excess IT equipment from the Navy Enterprise Resource Planning System once it receives a stamped DD 1348 from Naval Facilities Engineering Command's Property Disposal Office. In addition, the Property Management Team will continue to use the Naval Air Warfare Center Aircraft Division Excess Asset Form to ensure IT equipment is properly sanitized before release. According to the Commander of the Naval Air Warfare Center Aircraft Division, the required documentation takes years to be received from DRMS processing centers.

Our Response

The comments of the Navy Chief Information Officer and Commander of the Naval Air Warfare Center Aircraft Division were responsive on Recommendations 6.a, 6.b, and 6.c, and no additional comments are required. However, the comments on Recommendation 6.d were nonresponsive, for the following reasons.

The internal controls described by the Commander as having been instituted to implement Recommendation 6.d are the current procedures, rather than revised procedures. Therefore, the procedures as stated will continue to result in the same problems described in this report, problems that resulted in Recommendation 6.d.

If it removes excess IT equipment from the system when a stamped DD 1348 is received from the Naval Facilities Engineering Command Property Disposal Office, the Property Management Team will continue to remove excess IT equipment from the Navy Enterprise Resource Planning System prematurely, leaving equipment unaccounted for. The Property Disposal Office does not account for excess information technology equipment dropped off at its office, but merely operates as a holding facility and forwards equipment to the processing centers for disposal. Therefore, using documentation supplied by the Property Disposal Office to record disposal and removal of the IT equipment from the Navy Enterprise Resource Planning System is inaccurate and leaves the IT equipment unaccounted for until it reaches its final destination—the Defense Reutilization and Marketing Service. The Property Management Team is responsible for the management, tracking, reutilization, and disposition of all plant and minor property and for ensuring equipment is appropriately and accurately accounted for until disposal.

With regard to the Defense Reutilization and Marketing Service's processing centers' taking years to forward disposal information, the Web Enabled Document Conversion System (Web DOCS) was developed to provide electronic receipts for DOD Components. Web DOCS is a worldwide, Web-based system designed to provide an audit trail for DD 1348 documents. The system serves as the official record for turn-ins and is used to review and retrieve data and images. Customers can immediately retrieve an electronic image of a processed DD 1348. The Property Management Team can use Web DOCS to pull the required documentation for excess IT equipment and properly remove the equipment from the Navy Enterprise Resource Planning System.

We request that the Navy Chief Information Officer and the Commander of the Naval Air Warfare Center Aircraft Division reconsider their position on Recommendation 6.d and provide additional comments in response to the final report.

7. We recommend that the Commander, 436th Medical Group, Dover Air Force Base, and the Commander, 50th Space Communications Squadron, Schriever Air Force Base:

a. Account for all hard drives removed from their computer shells.

b. Account for hard drives removed from their computer shells that contain sensitive information in an electronic record-keeping system as required by DOD Instruction 5000.64, "Accountability and Management of DOD Owned Equipment and Other Accountable Property," November 2, 2006.

Management Comments Required

The Commander, 436th Medical Group, Dover Air Force Base, and the Commander, 50th Space Communications Squadron, Schriever Air Force Base, did not provide comments on the draft report. We request that the Commanders provide comments on the final report.

Appendix A. Scope and Methodology

We conducted this performance audit from November 2007 through June 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We conducted this audit to determine whether DOD sanitized and disposed of excess unclassified IT equipment in accordance with Federal and DOD requirements. We tested the following to answer the audit objective.

- Information Security: We determined whether DOD Components had properly sanitized and properly prepared documentation for the excess IT equipment before forwarding it to the DRMS processing centers. In addition, we determined whether DRMS processing centers confirmed proper documentation of excess IT equipment before processing it. We used the Disposition Memorandum as the criteria to evaluate the internal control related to information security.

- Physical Security: We determined whether DOD Components and the DRMS processing centers implemented appropriate internal controls to protect equipment from pilferage. We used DOD Instruction 5200.08-R, "Physical Security Program," April 9, 2007 as the criteria to evaluate the internal control related to physical security.

- Property Accountability: We determined whether DOD Components and DRMS processing centers properly accounted for IT equipment throughout its life cycle. We used DOD Instruction 5000.64 as the criteria to evaluate the internal control related to property accountability.

We accomplished the audit in two phases. In the first phase, we determined whether the DRMS disposed of excess unclassified IT equipment in accordance with DOD requirements. During this phase we visited DRMS headquarters, nine DRMS processing centers, and two DRMS contractors' locations from January through March 2008. In the second phase, we determined whether DOD Components properly safeguarded sensitive information residing on excess DOD IT equipment by properly sanitizing and accounting for IT equipment before forwarding it to DRMS.

From June through July 2008, we visited six DOD Components:

- USACE Louisville District;
- NAS Patuxent River;
- 436th Medical Group, Dover AFB;
- 108th Air Refueling Wing, McGuire AFB;
- 21st Space Wing Command, Peterson AFB, Colorado; and
- 50th Space Communications Squadron, Schriever AFB.

We selected a non-statistical sample of 543 out of 4,105 pieces of excess unclassified IT equipment. The sample included laptop hard drives, desktop hard drives, digital systems, and an electrocardiogram machine. To evaluate the controls exercised over excess DOD IT equipment at each DOD Component, we reviewed inventory records and sanitization and disposition documentation, and we interviewed personnel with DRMS and other DOD organizations. In addition, using forensic software we tested excess hard drives to ensure that all data had been removed. If not, we determined what type of data remained. During Phase I, however, we tested hard drives at only two of the nine DRMS processing centers because of lack of testing equipment. Finally, we evaluated the sufficiency of physical controls over the excess IT equipment at each location visited.

Use of Computer-Processed Data

We relied on computer-processed data extracted from the Defense Reutilization and Marketing Automated Information System, Management Information Distribution and Access System, Asset Inventory Management System, and the Automated Personal Property Management System. We did not find significant errors between the computer-processed data and source documents that would preclude use of the computer-processed data to meet the audit objectives or that would change the conclusions in this report.

Through existence and completion testing, we determined that the Defense Reutilization and Marketing Automated Information System, Management Information Distribution and Access System, Asset Inventory Management System, and Automated Personal Property Management System data sources reliable. We did not perform tests on the controls in place for the system, but validated the accuracy of the data extracted from each system with other documentation and the results of our existence and completion testing (book-to-floor and floor-to-book tests).

Use of Technical Assistance

We obtained technical assistance from two IT specialists from the DOD Office of Inspector General, Information Systems Directorate. The IT specialists accompanied the audit team to the Mechanicsburg and Wright-Patterson DRMS processing centers and to Dover AFB to test processed DOD unclassified hard drives. For the remaining sites, the

Information Systems Directorate provided the audit team with IT forensic equipment and hands-on training to test hard drives to determine whether equipment still contained readable information. If information was found on a piece of equipment, the IT specialist analyzed the information to determine whether it was readable and what type of information it was.

Prior Coverage

During the last 5 years, the Department of Defense Office of Inspector General (DOD IG), Naval Audit Service, and the Air Force Audit Agency have issued four reports discussing sanitizing, disposing of, and accounting for excess IT equipment in accordance with Federal and DOD security and environmental laws and regulations. Unrestricted DOD IG reports can be accessed at http://www.DODig.mil/Audit/reports/index.html. Air Force Audit Agency reports can be accessed from .mil domains over the Internet at https://afkm.wpafb.af.mil/ASPs/CoP/OpenCoP.asp?Filter=OO-AD-01-41 by those with Common Access Cards.

DOD IG

DOD Report No. D-2008-114, “Accountability for Defense Security Service Assets With Personally Identifiable Information,” July 24, 2008

Naval Audit Service

Report No. N2009-0014, “Control over Wireless Devices at Selected Commander, Navy Installations Command and Naval Facilities Engineering Command Activities,” December 17, 2008 (For Official Use Only)

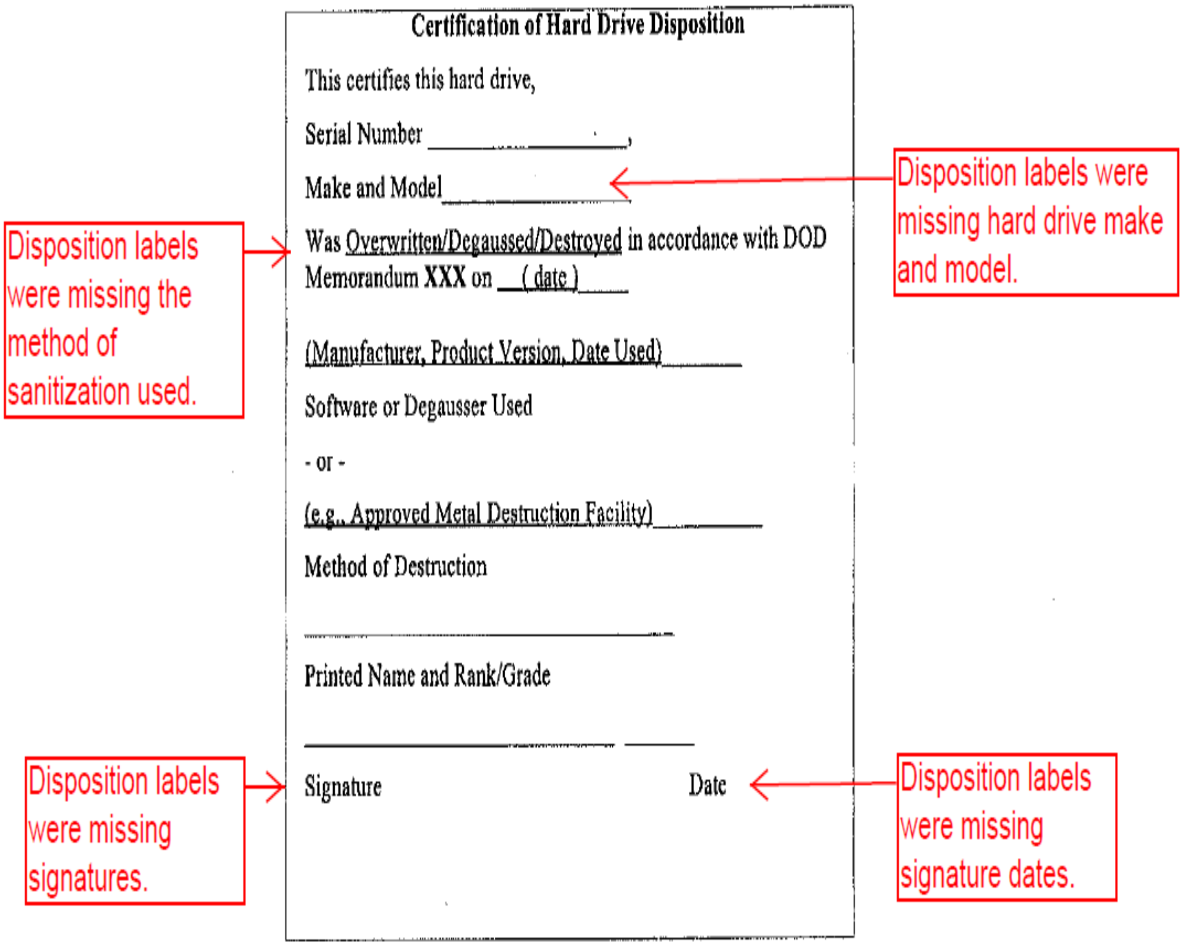
Report No N2009-0027, “Processing of Computers and Hard Drives During the Navy Marine Corps Intranet (NMCI) Computer Disposal Process,” April 28, 2009 (For Official Use Only)

Air Force Audit Agency

Air Force Audit Agency Report No. F2005-0008-FC4000, “Demilitarization Process,” September 8, 2005

Appendix B. Label Certifying Hard Drive Disposition

DOD Components are required by the Disposition Memorandum to complete and attach the Certification of Hard Drive Disposition label to the hard drive or the computer housing the hard drive. The signed label certifies that the hard drive has no readable information on it. We have indicated examples of the types of information missing from the labels included in our review.



Certification of Hard Drive Disposition

This certifies this hard drive,

Serial Number ______________,

Make and Model______________

Was Overwritten/Degaussed/Destroyed in accordance with DOD Memorandum **XXX** on __(date)____

(Manufacturer, Product Version, Date Used)________

Software or Degausser Used

- or -

(e.g., Approved Metal Destruction Facility)________

Method of Destruction

____

Printed Name and Rank/Grade

______________________________ ________

Signature Date

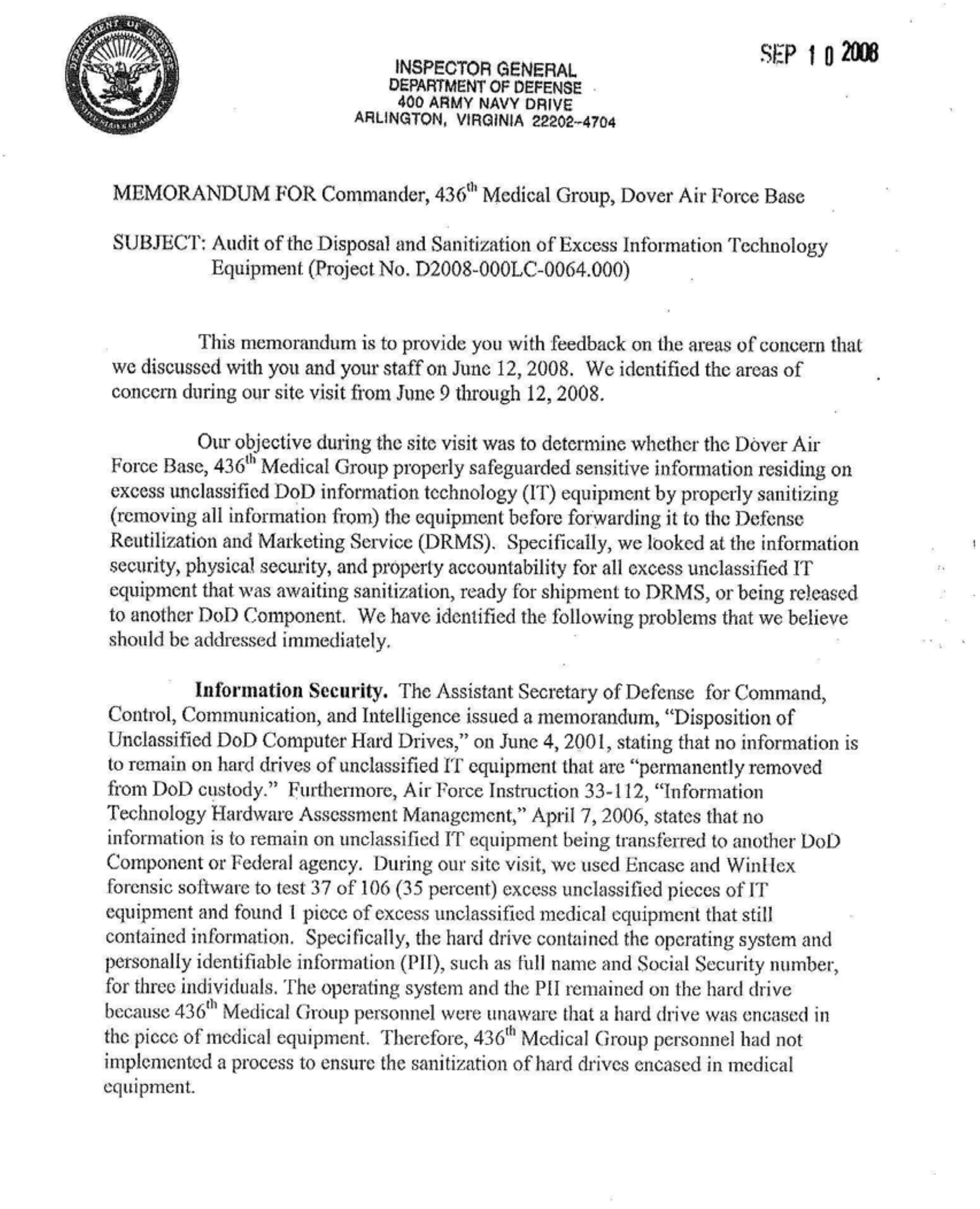
Disposition labels were missing hard drive make and model.

Disposition labels were missing the method of sanitization used.

Disposition labels were missing signatures.

Disposition labels were missing signature dates.

Appendix C. Immediate Action Memoranda to DOD Components



SEP 1 0 2008

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

MEMORANDUM FOR Commander, 436th Medical Group, Dover Air Force Base

SUBJECT: Audit of the Disposal and Sanitization of Excess Information Technology Equipment (Project No. D2008-000LC-0064.000)

This memorandum is to provide you with feedback on the areas of concern that we discussed with you and your staff on June 12, 2008. We identified the areas of concern during our site visit from June 9 through 12, 2008.

Our objective during the site visit was to determine whether the Dover Air Force Base, 436th Medical Group properly safeguarded sensitive information residing on excess unclassified DoD information technology (IT) equipment by properly sanitizing (removing all information from) the equipment before forwarding it to the Defense Reutilization and Marketing Service (DRMS). Specifically, we looked at the information security, physical security, and property accountability for all excess unclassified IT equipment that was awaiting sanitization, ready for shipment to DRMS, or being released to another DoD Component. We have identified the following problems that we believe should be addressed immediately.

Information Security. The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence issued a memorandum, "Disposition of Unclassified DoD Computer Hard Drives," on June 4, 2001, stating that no information is to remain on hard drives of unclassified IT equipment that are "permanently removed from DoD custody." Furthermore, Air Force Instruction 33-112, "Information Technology Hardware Assessment Management," April 7, 2006, states that no information is to remain on unclassified IT equipment being transferred to another DoD Component or Federal agency. During our site visit, we used Encase and WinHex forensic software to test 37 of 106 (35 percent) excess unclassified pieces of IT equipment and found 1 piece of excess unclassified medical equipment that still contained information. Specifically, the hard drive contained the operating system and personally identifiable information (PII), such as full name and Social Security number, for three individuals. The operating system and the PII remained on the hard drive because 436th Medical Group personnel were unaware that a hard drive was encased in the piece of medical equipment. Therefore, 436th Medical Group personnel had not implemented a process to ensure the sanitization of hard drives encased in medical equipment.

The evidence that we found illustrates that excess unclassified hard drives encased in medical equipment were not properly sanitized before being sent to another DoD Component or Federal agency. Therefore, the 436th Medical Group reduces the assurance that PII or other sensitive DoD information stored on medical equipment will be protected from unauthorized release.

Recommendation. We recommend that the Commander, 436th Medical Group (1) conduct an evaluation of all medical equipment on which patient-specific information is entered to determine whether the medical equipment contains a hard drive and (2) develop a process to ensure proper sanitization of all medical equipment that contains a hard drive.

We are providing you these interim results so that you may take appropriate action. We performed this audit in accordance with generally accepted government auditing standards. We are continuing the subject audit and will issue a draft report upon completion of the audit incorporating these interim results and actions taken. If you have questions, please contact me at [redacted]

Rhonda L. Ragsdale

Rhonda L. Ragsdale
Acting Program Director
Readiness and Operations Support

cc:
Air Force Office of Warfighting Integration and Chief Information Officer
(Attn:SAF/XCDI)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

NOV 21 2008

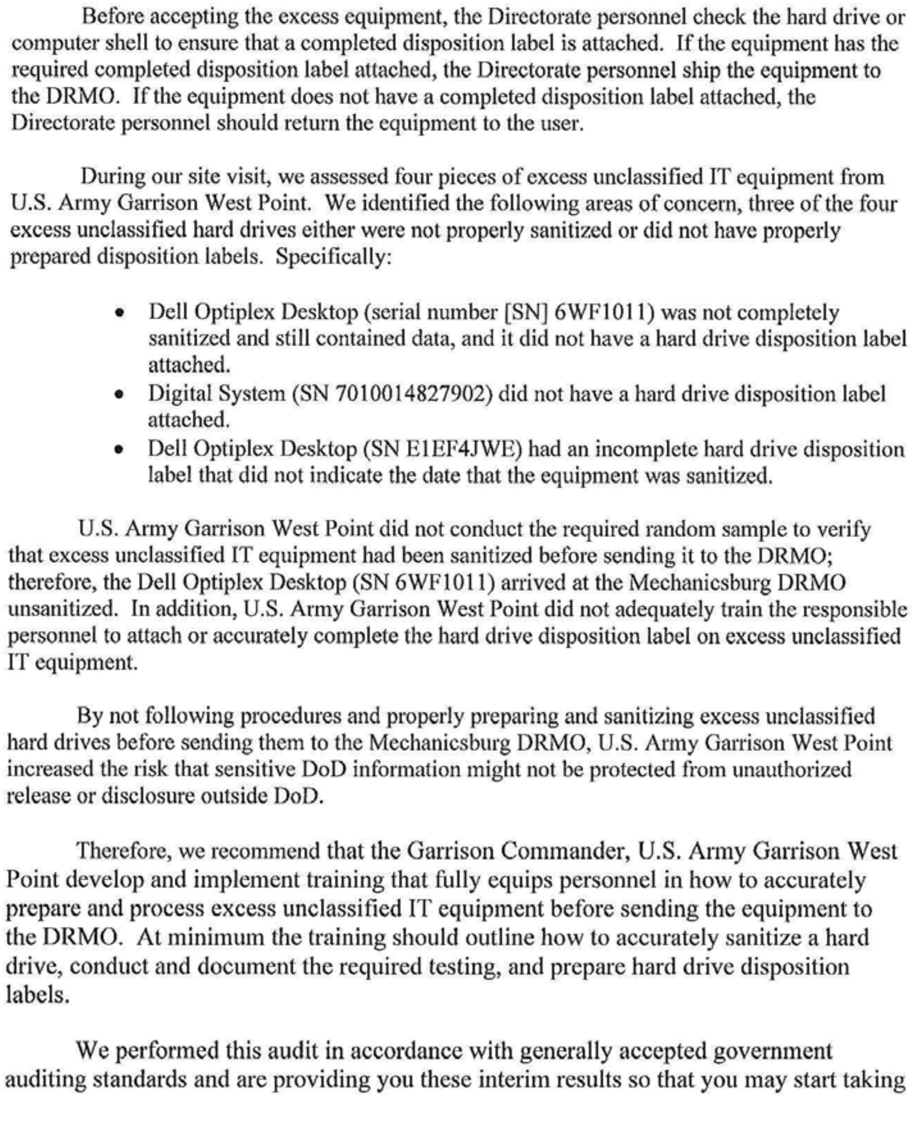
MEMORANDUM FOR GARRISON COMMANDER, U.S. ARMY GARRISON WEST POINT
DIRECTOR OF LOGISTICS, U.S. ARMY GARRISON WEST POINT
DIRECTOR OF INFORMATION MANAGEMENT, U.S. ARMY GARRISON WEST POINT

SUBJECT: Audit of the Disposal and Sanitization of Excess Information Technology Equipment (Project No. D2008-D000LC-0064.000)

During our site visit to the Defense Reutilization and Marketing Office (DRMO) in Mechanicsburg, PA, on February 7, 2008, we found excess equipment sent from U.S. Army Garrison West Point that did not meet disposition regulations. From February 2008 until August 2008 we worked closely with the Defense Reutilization and Marketing Service and the U.S. Army Network Enterprise Technology Command to identify that the excess equipment belonged to the U.S. Army Garrison West Point. Our objective during the site visit was to determine whether the DRMOs were disposing of excess information technology (IT) equipment in accordance with DoD security regulations. Specifically, we looked at the information security; physical security; and property accountability of all excess unclassified IT equipment that were waiting to be processed by the Mechanicsburg DRMO, processed by the Mechanicsburg DRMO, or waiting to be returned to a DoD activity (because the excess unclassified IT equipment did not have the appropriate documentation). We are providing this memorandum prior to our report for your consideration in taking appropriate action.

The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence, issued a memorandum, "Disposition of Unclassified DoD Computer Hard Drives," on June 4, 2001, stating that no information is to remain on hard drives of unclassified IT equipment that is "permanently removed from DoD custody." The memorandum also requires that a signed disposition label identifying the method of sanitization be attached to the hard drive or the computer housing the hard drive after sanitization. If overwriting is the chosen sanitization method, the memorandum recommends that a trained individual that did not participate in the overwriting process conduct a random sample of at least 20 percent of the sanitized equipment.

Currently, when an activity at the U.S. Army Garrison West Point determines IT equipment is excess or obsolete, the information management officer uses the authorized overwriting software on the hard drive of each system. Once the excess unclassified IT equipment is sanitized, the information management officer prepares the hard drive disposition label and attaches it to the equipment. The hand receipt holder or property manager for each activity prepares the required turn-in documentation and arranges for the equipment to be turned in to the Directorate of Logistics.



Before accepting the excess equipment, the Directorate personnel check the hard drive or computer shell to ensure that a completed disposition label is attached. If the equipment has the required completed disposition label attached, the Directorate personnel ship the equipment to the DRMO. If the equipment does not have a completed disposition label attached, the Directorate personnel should return the equipment to the user.

During our site visit, we assessed four pieces of excess unclassified IT equipment from U.S. Army Garrison West Point. We identified the following areas of concern, three of the four excess unclassified hard drives either were not properly sanitized or did not have properly prepared disposition labels. Specifically:

- Dell Optiplex Desktop (serial number [SN] 6WF1011) was not completely sanitized and still contained data, and it did not have a hard drive disposition label attached.
- Digital System (SN 7010014827902) did not have a hard drive disposition label attached.
- Dell Optiplex Desktop (SN E1EF4JWE) had an incomplete hard drive disposition label that did not indicate the date that the equipment was sanitized.

U.S. Army Garrison West Point did not conduct the required random sample to verify that excess unclassified IT equipment had been sanitized before sending it to the DRMO; therefore, the Dell Optiplex Desktop (SN 6WF1011) arrived at the Mechanicsburg DRMO unsanitized. In addition, U.S. Army Garrison West Point did not adequately train the responsible personnel to attach or accurately complete the hard drive disposition label on excess unclassified IT equipment.

By not following procedures and properly preparing and sanitizing excess unclassified hard drives before sending them to the Mechanicsburg DRMO, U.S. Army Garrison West Point increased the risk that sensitive DoD information might not be protected from unauthorized release or disclosure outside DoD.

Therefore, we recommend that the Garrison Commander, U.S. Army Garrison West Point develop and implement training that fully equips personnel in how to accurately prepare and process excess unclassified IT equipment before sending the equipment to the DRMO. At minimum the training should outline how to accurately sanitize a hard drive, conduct and document the required testing, and prepare hard drive disposition labels.

We performed this audit in accordance with generally accepted government auditing standards and are providing you these interim results so that you may start taking appropriate corrective actions. In January 2009, we anticipate issuing the draft report formally outlining the above stated recommendation for your comment. We would like to give you credit in both the draft and final reports for any corrective action taken as a result of this memorandum. Therefore, we request that you keep us abreast of all corrective actions you take or have taken to address the recommendation. Please send your corrective actions (in electronic format) to me at [redacted]

Rhonda L. Ragsdale

Rhonda L. Ragsdale
Acting Program Director
Readiness, Operations, and Support

cc: Director, Army NETCOM Information Assurance and Compliance

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

NOV 21 2008

MEMORANDUM FOR COMMANDER, 108TH AIR REFUELING WING
COMMANDER, 108TH COMMUNICATIONS FLIGHT
COMMANDER, 108TH LOGISTIC READINESS SQUADRON

SUBJECT: Audit of the Disposal and Sanitization of Excess Information Technology Equipment (Project No. D2008-D000LC-0064)

This memorandum is to provide you with feedback on the areas of concern that we discussed with you and your staff on July 10, 2008. We identified the areas of concern during our site visit from July 8 through 10, 2008.

Our objective during the visit was to determine whether the McGuire Air Force Base, 108th Air Refueling Wing (ARW) properly safeguarded sensitive information residing on excess unclassified DoD information technology (IT) equipment by properly sanitizing (removing all information from) the equipment before forwarding it to the Defense Reutilization and Marketing Service (DRMS). Specifically, we looked at the information security, physical security, and property accountability for all excess unclassified IT equipment that was awaiting sanitization, ready for shipment to DRMS, or being released to another DoD Component. We are providing this memorandum prior to our report for your consideration in taking appropriate action.

DoD Instruction 5000.64, "Accountability and Management of the DoD-Owned Equipment and Other Accountable Property," November 2, 2006, requires that an electronic record of the receipt of property be maintained throughout its life cycle regardless of its status (unserviceable, obsolete, excess, surplus) or physical location. Furthermore, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence memorandum on the "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001 (the Disposition Memorandum), and Air Force System Security Instruction 5020, "Remanence Security," April 17, 2003, state that a signed hard drive disposition label identifying the method of sanitization be attached to the hard drive or the computer housing the hard drive after sanitization.

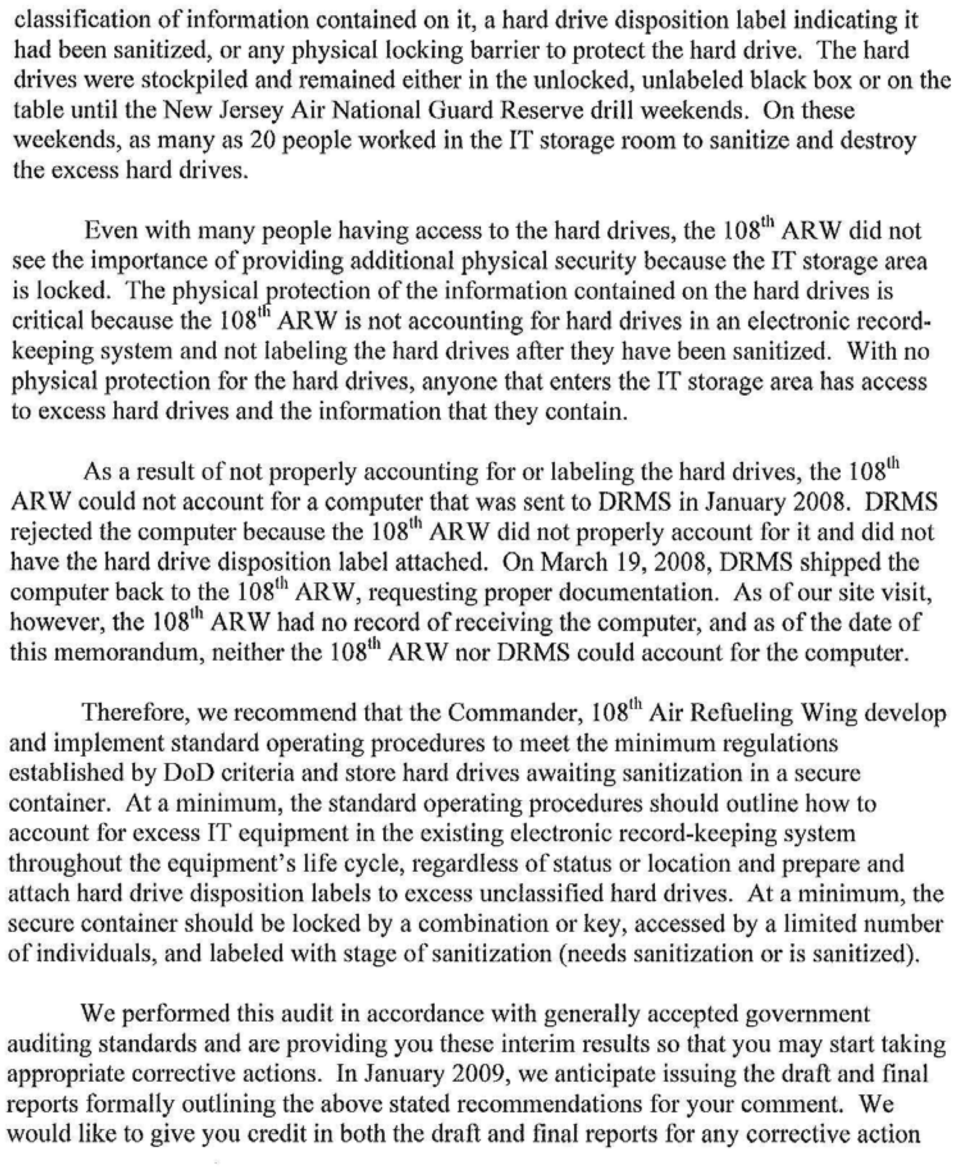
Through the observations we made and data we gathered, we concluded that the 108th ARW did not properly account for or attach proper documentation to its excess unclassified IT equipment. Therefore, DoD cannot ensure that information remaining on hard drives is sanitized and then properly disposed of.

Property Accountability. The 108th ARW was not accounting for excess unclassified IT equipment in an electronic record-keeping system. Specifically, personnel did not account for 41 computer shells and 51 hard drives found in the IT storage area in an electronic record-keeping system. DoD Instruction 5000.64 requires that excess unclassified IT equipment be accounted for in an electronic record-keeping system until receipt of written confirmation from the entity receiving the equipment. The 92 pieces of excess unclassified IT equipment were removed from the electronic record-keeping system when the equipment was turned into the Communications Flight Unit for sanitization and disposal instead of when DRMS received and processed the equipment. We were unable to determine how long the 41 computer shells and 51 hard drives had been waiting in the IT storage area because they were not tracked in the electronic record-keeping system.

The 108th ARW personnel did not see the importance of accounting for the unclassified IT equipment after it was designated excess, and they were not aware that DoD Instruction 5000.64 requires accountability for property throughout its life cycle. Properly tracking the excess IT equipment in an electronic record-keeping system would allow the 108th ARW to determine on-hand inventory levels, the physical location of equipment (warehouse, in-transit, or DRMS), and the original user of all excess unclassified IT equipment as well as the type of information it contains.

Hard Drive Disposition Labels. The 108th ARW did not attach hard drive disposition labels to sanitized hard drives or fully complete the hard drive disposition labels on computer shells. Specifically, of the 51 hard drives on hand during our visit, none had a hard drive disposition label. To determine whether the 108th ARW had properly sanitized the hard drives, we tested three and determined that it had properly sanitized them. In addition, 41 computer shells had hard drive disposition labels, but the labels did not indicate the method of sanitization. The 108th ARW did not attach or fully complete the hard drive disposition label because personnel were not familiar with the Disposition Memorandum or with Air Force System Security Instruction 5020, which requires completed hard drive disposition labels to be attached to the sanitized hard drive or to the computer shell housing the hard drive.

Physical Security. The 108th ARW did not physically protect the excess hard drives that were removed from the excess computer shells. Specifically, we observed 42 excess hard drives stored in an unlocked and unlabeled black box on the floor of the IT storage room, and an additional excess nine hard drives stored on a table near the overwriting machine. Of the 51 excess hard drives, not one had any indication of the



classification of information contained on it, a hard drive disposition label indicating it had been sanitized, or any physical locking barrier to protect the hard drive. The hard drives were stockpiled and remained either in the unlocked, unlabeled black box or on the table until the New Jersey Air National Guard Reserve drill weekends. On these weekends, as many as 20 people worked in the IT storage room to sanitize and destroy the excess hard drives.

Even with many people having access to the hard drives, the 108th ARW did not see the importance of providing additional physical security because the IT storage area is locked. The physical protection of the information contained on the hard drives is critical because the 108th ARW is not accounting for hard drives in an electronic record-keeping system and not labeling the hard drives after they have been sanitized. With no physical protection for the hard drives, anyone that enters the IT storage area has access to excess hard drives and the information that they contain.

As a result of not properly accounting for or labeling the hard drives, the 108th ARW could not account for a computer that was sent to DRMS in January 2008. DRMS rejected the computer because the 108th ARW did not properly account for it and did not have the hard drive disposition label attached. On March 19, 2008, DRMS shipped the computer back to the 108th ARW, requesting proper documentation. As of our site visit, however, the 108th ARW had no record of receiving the computer, and as of the date of this memorandum, neither the 108th ARW nor DRMS could account for the computer.

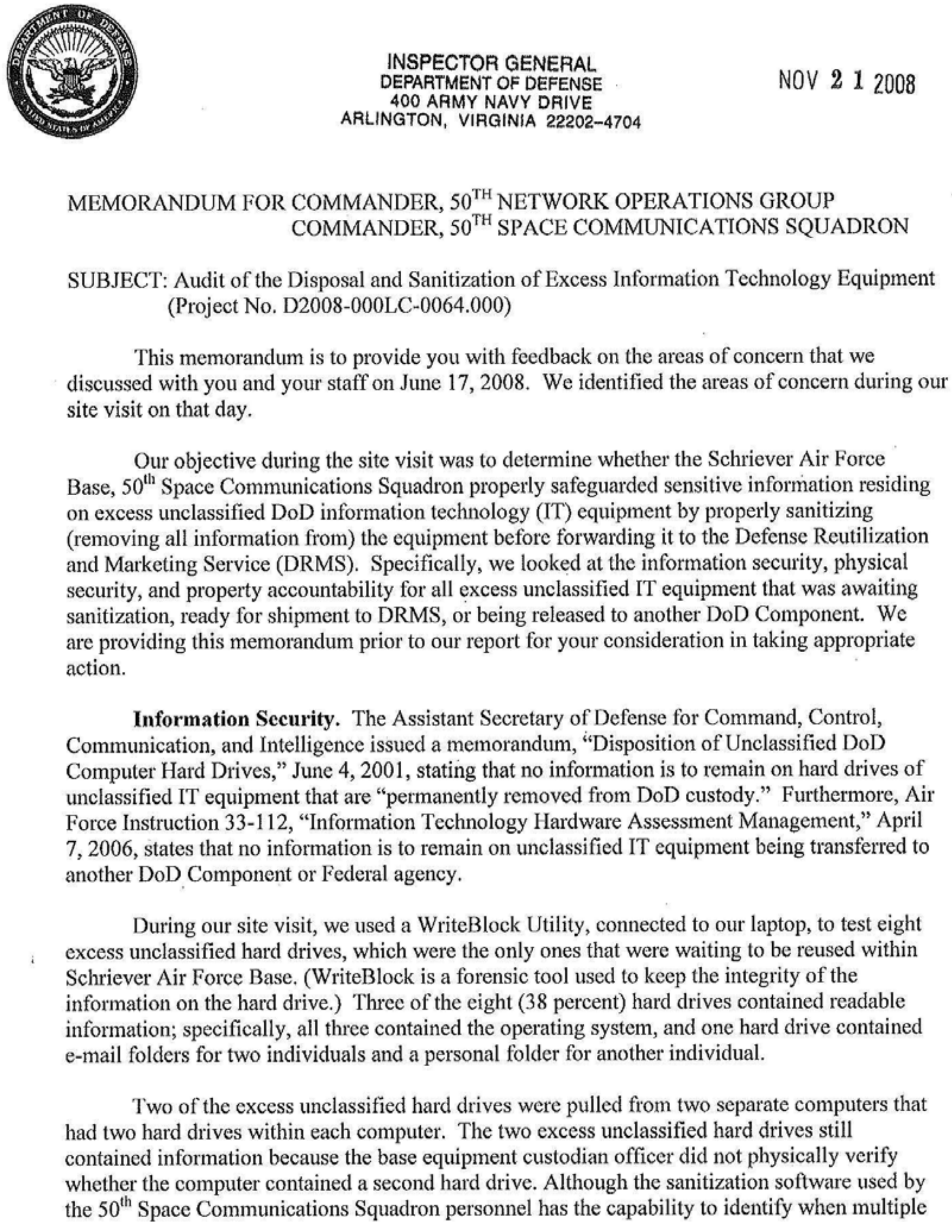
Therefore, we recommend that the Commander, 108th Air Refueling Wing develop and implement standard operating procedures to meet the minimum regulations established by DoD criteria and store hard drives awaiting sanitization in a secure container. At a minimum, the standard operating procedures should outline how to account for excess IT equipment in the existing electronic record-keeping system throughout the equipment's life cycle, regardless of status or location and prepare and attach hard drive disposition labels to excess unclassified hard drives. At a minimum, the secure container should be locked by a combination or key, accessed by a limited number of individuals, and labeled with stage of sanitization (needs sanitization or is sanitized).

We performed this audit in accordance with generally accepted government auditing standards and are providing you these interim results so that you may start taking appropriate corrective actions. In January 2009, we anticipate issuing the draft and final reports formally outlining the above stated recommendations for your comment. We would like to give you credit in both the draft and final reports for any corrective action taken as a result of this memorandum. Therefore, we request that you keep us abreast of all corrective actions you take or have taken to address the recommendations. Please send your corrective actions (in electronic format) to me at [redacted]

Rhonda L. Ragsdale

Rhonda L. Ragsdale
Acting Program Director
Readiness, Operations, and Support

cc: Air Force Office of Warfighting Integration and Chief Information Officer
(Attn: SAF/XCDI)



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

NOV 21 2008

MEMORANDUM FOR COMMANDER, 50TH NETWORK OPERATIONS GROUP
COMMANDER, 50TH SPACE COMMUNICATIONS SQUADRON

SUBJECT: Audit of the Disposal and Sanitization of Excess Information Technology Equipment (Project No. D2008-000LC-0064.000)

This memorandum is to provide you with feedback on the areas of concern that we discussed with you and your staff on June 17, 2008. We identified the areas of concern during our site visit on that day.

Our objective during the site visit was to determine whether the Schriever Air Force Base, 50th Space Communications Squadron properly safeguarded sensitive information residing on excess unclassified DoD information technology (IT) equipment by properly sanitizing (removing all information from) the equipment before forwarding it to the Defense Reutilization and Marketing Service (DRMS). Specifically, we looked at the information security, physical security, and property accountability for all excess unclassified IT equipment that was awaiting sanitization, ready for shipment to DRMS, or being released to another DoD Component. We are providing this memorandum prior to our report for your consideration in taking appropriate action.

Information Security. The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence issued a memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, stating that no information is to remain on hard drives of unclassified IT equipment that are "permanently removed from DoD custody." Furthermore, Air Force Instruction 33-112, "Information Technology Hardware Assessment Management," April 7, 2006, states that no information is to remain on unclassified IT equipment being transferred to another DoD Component or Federal agency.

During our site visit, we used a WriteBlock Utility, connected to our laptop, to test eight excess unclassified hard drives, which were the only ones that were waiting to be reused within Schriever Air Force Base. (WriteBlock is a forensic tool used to keep the integrity of the information on the hard drive.) Three of the eight (38 percent) hard drives contained readable information; specifically, all three contained the operating system, and one hard drive contained e-mail folders for two individuals and a personal folder for another individual.

Two of the excess unclassified hard drives were pulled from two separate computers that had two hard drives within each computer. The two excess unclassified hard drives still contained information because the base equipment custodian officer did not physically verify whether the computer contained a second hard drive. Although the sanitization software used by the 50th Space Communications Squadron personnel has the capability to identify when multiple hard drives are encased in a computer, in this situation, the software was unable to detect these hard drives. We were unable to determine why the third hard drive contained information.

The evidence that we found illustrated that the 50th Space Communications Squadron did not properly sanitize excess unclassified hard drives before sending them to another DoD Component or Federal agency. Therefore, the 50th Space Communications Squadron increases the risk that DoD information is not fully protected from unauthorized release.

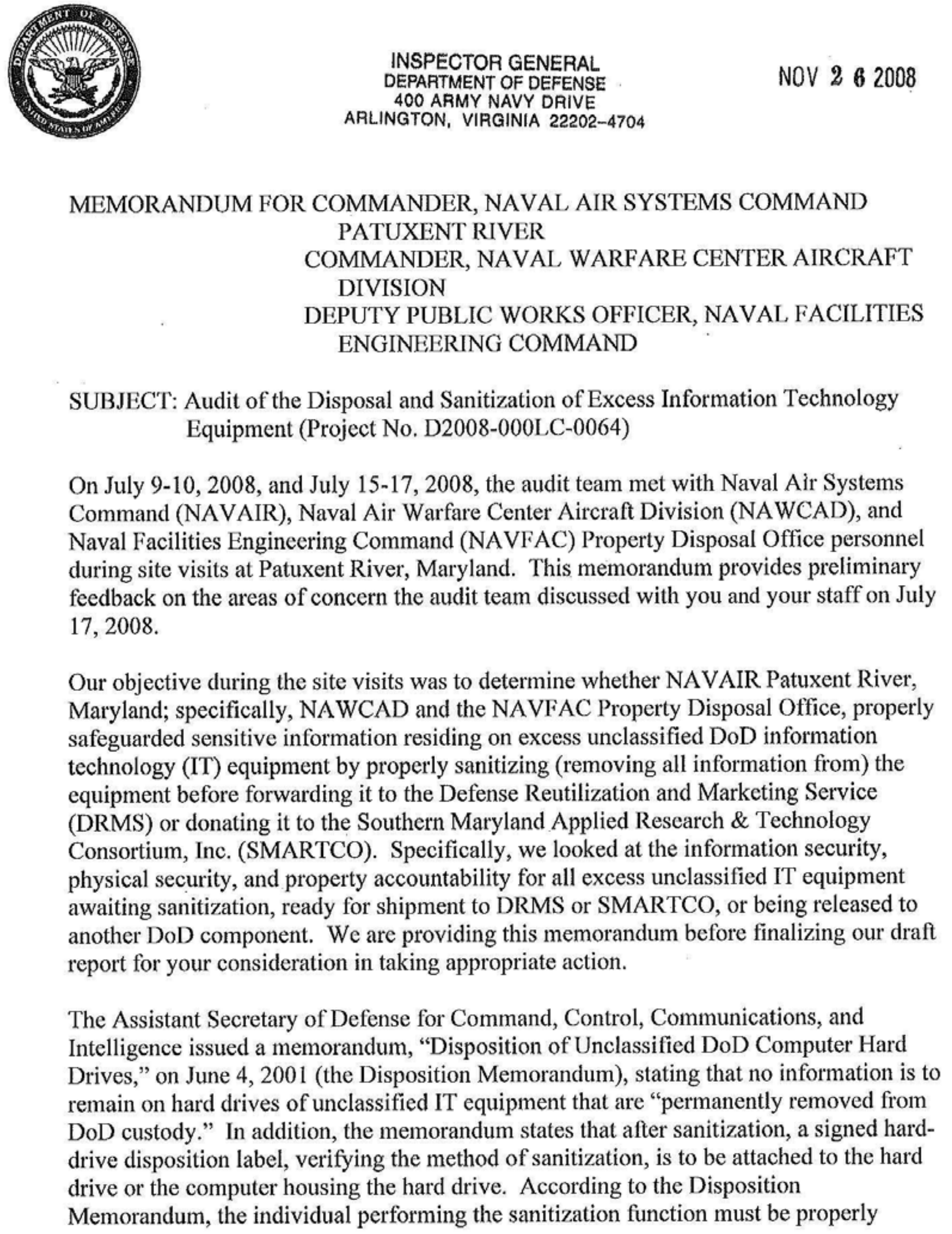
Therefore, we recommend that the Commander, 50th Space Communications Squadron physically verify the number of hard drives encased in the excess unclassified IT equipment; provide equipment custodians hands-on training on the use of the sanitization software; and develop and implement uniform standard operating procedures for Schriever Air Force Base to properly sanitize excess unclassified IT equipment. At a minimum, the standard operating procedures should clearly define the roles and responsibilities of all personnel involved in the sanitization of hard drives and describe the Schriever Air Force Base sanitization process, detailing the sanitization software used and the physical verification process.

We performed this audit in accordance with generally accepted government auditing standards and are providing you these interim results so that you may start taking appropriate corrective actions. In January 2009, we anticipate issuing the draft report formally outlining the above stated recommendation for your comment. We would like to give you credit in both the draft and final reports for any corrective action taken as a result of this memorandum. Therefore, we request that you keep us abreast of all corrective actions you take or have taken to address the recommendation. Please send your corrective actions (in electronic format) to me at [redacted]

Rhonda L. Ragsdale

Rhonda L. Ragsdale
Acting Program Director
Readiness, Operations, and Support

cc: Air Force Office of Warfighting Integration and Chief Information Officer
(Attn: SAF/XCDI)



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

NOV 2 6 2008

MEMORANDUM FOR COMMANDER, NAVAL AIR SYSTEMS COMMAND
PATUXENT RIVER
COMMANDER, NAVAL WARFARE CENTER AIRCRAFT
DIVISION
DEPUTY PUBLIC WORKS OFFICER, NAVAL FACILITIES
ENGINEERING COMMAND

SUBJECT: Audit of the Disposal and Sanitization of Excess Information Technology Equipment (Project No. D2008-000LC-0064)

On July 9-10, 2008, and July 15-17, 2008, the audit team met with Naval Air Systems Command (NAVAIR), Naval Air Warfare Center Aircraft Division (NAWCAD), and Naval Facilities Engineering Command (NAVFAC) Property Disposal Office personnel during site visits at Patuxent River, Maryland. This memorandum provides preliminary feedback on the areas of concern the audit team discussed with you and your staff on July 17, 2008.

Our objective during the site visits was to determine whether NAVAIR Patuxent River, Maryland; specifically, NAWCAD and the NAVFAC Property Disposal Office, properly safeguarded sensitive information residing on excess unclassified DoD information technology (IT) equipment by properly sanitizing (removing all information from) the equipment before forwarding it to the Defense Reutilization and Marketing Service (DRMS) or donating it to the Southern Maryland Applied Research & Technology Consortium, Inc. (SMARTCO). Specifically, we looked at the information security, physical security, and property accountability for all excess unclassified IT equipment awaiting sanitization, ready for shipment to DRMS or SMARTCO, or being released to another DoD component. We are providing this memorandum before finalizing our draft report for your consideration in taking appropriate action.

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence issued a memorandum, "Disposition of Unclassified DoD Computer Hard Drives," on June 4, 2001 (the Disposition Memorandum), stating that no information is to remain on hard drives of unclassified IT equipment that are "permanently removed from DoD custody." In addition, the memorandum states that after sanitization, a signed hard-drive disposition label, verifying the method of sanitization, is to be attached to the hard drive or the computer housing the hard drive. According to the Disposition Memorandum, the individual performing the sanitization function must be properly trained and certified, and this individual will be responsible for certifying that the process has been successfully completed.

Further, Naval Air Station, Patuxent River Instruction 4010.1F, "Disposition of Excess Personal Property and Salvageable Scrap," December 21, 1999, requires that a disposal turn-in document (DD Form 1348-A) be used to turn equipment over to DRMS for reutilization, transfer, donation, or sale. Also, the Department of the Navy Information Assurance Remanence Security Publication 5239-26, May 2000, states that operational and nonoperational magnetic data storage media should be degaussed with National Security Agency (NSA)-approved degaussing equipment.

During earlier visits to DRMS, we identified weaknesses within the NAVAIR Patuxent River Aircraft Division property disposal process. Specifically, NAWCAD personnel had generated and submitted duplicate disposal turn-in document numbers (N0042172750012) to DRMS. This occurred because NAWCAD personnel were generating disposal turn-in document numbers using different means and, in some cases, manually generating disposal turn-in document numbers.

NAVAIR personnel should use the Web based Electronic Turn-in Document (ETID) system, which is an electronic method for preparing a disposal turn-in document. The ETID system was developed by DRMS to simplify and improve the turn-in process. As a result of this deficiency, we visited and reviewed the sanitization and disposal process for the following Navy activities at Patuxent River:

- NAWCAD Property Management Team,
- NAWCAD Air Combat Environment Test and Evaluation Facility Lab,
- NAWCAD E-6B Systems Integration Lab,
- NAWCAD 7.2.4 Data Center,
- NAVAIR 6.8.4 Data Center,
- Space and Naval Warfare Systems Command (SPAWAR) Configuration Management Lab, and
- NAVFAC Property Disposal Office, which is responsible for forwarding all excess equipment to DRMS.

Disposal and Sanitization Process. At Patuxent River, the NAVAIR labs, NAVAIR data centers, NAWCAD Property Management Team, and NAVFAC Property Disposal Office are involved in processing excess unclassified IT equipment. NAVAIR labs and data centers generating excess IT equipment must ensure that all equipment forwarded to the NAWCAD Property Management Team or the NAVFAC Property Disposal Office is properly sanitized. Some labs and data centers forward excess IT equipment to the NAWCAD Property Management Team for processing, and others forward equipment directly to the NAVFAC Property Disposal Office. Before forwarding excess IT equipment, some labs and data centers physically remove hard drives. Physically removed hard drives are degaussed, overwritten, or sent to NSA for destruction. Equipment received by the NAWCAD Property Management Team is processed and forwarded to the NAVFAC Property Disposal Office. All equipment received by the NAVFAC Property Disposal Office is turned in to DRMS.

Results of Patuxent River, Maryland, Review. Through our observations and data gathered at NAWCAD, SPAWAR, and the NAVFAC Property Disposal Office, we identified a general lack of consistency in how labs and data centers sanitized and processed excess IT equipment for disposal. We concluded that the NAVAIR personnel did not properly sanitize or complete appropriate documentation for their unclassified IT equipment before it was released to other DoD, Federal, or non-Federal organizations. Therefore, NAVAIR increased the risk that unclassified or sensitive DoD information may not be protected from unauthorized release or disclosure outside DoD.

Information Security. NAVAIR did not properly sanitize or complete appropriate documentation because personnel responsible for sanitization and disposal did not follow or were not aware of established policies. In addition, personnel responsible for sanitizing were not properly trained to perform the sanitization function. During our site visit, we found five of seven (71 percent) pieces of excess unclassified equipment that still contained information. Specifically, we found that two of the three NAWCAD hard drives at the NAVFAC Property Disposal Office and three of the four SPAWAR hard drives at the NAWCAD Property Management Team warehouse still contained readable information. The computers housed at the NAVFAC Property Disposal Office did not contain any documentation supporting their sanitization. Further, the documentation with the computers housed at the NAWCAD Property Management warehouse was incomplete.

Approved Sanitization Equipment. We also saw that NAWCAD personnel were not using NSA-approved degaussers as required. In fact, in one instance, NAWCAD E-6B Systems Integration Lab personnel used an audio/video degausser, which is not designed to degauss hard drives, but rather, videotape cassettes.

As a result of these deficiencies, NAVAIR, NAWCAD, SPAWAR, and NAVFAC cannot ensure that excess unclassified IT equipment is protected from unauthorized release. Therefore, we recommend that NAVAIR and the NAWCAD Commander, Patuxent River, Maryland, in conjunction with the NAVFAC Public Works Officer develop and implement written policies and procedures to effectively sanitize and process excess unclassified IT equipment. The written policies and procedures should clearly define:

- the roles and responsibilities for all Patuxent River personnel responsible for sanitization and disposal,

- the use of only NSA-approved sanitization equipment to properly overwrite and degauss excess unclassified IT equipment, and
- training for all personnel in how to accurately prepare and process excess unclassified IT equipment before forwarding it to DRMO.

We also recommend that NAVAIR and the NAWCAD Commander, Patuxent River, Maryland, ensure that only the ETID system is used to generate disposal turn-in documents.

We performed this audit in accordance with generally accepted government auditing standards. We are providing you these interim results so that you may start taking appropriate corrective actions.

Early in 2009, we anticipate issuing the draft report, formally outlining the above-stated recommendations for your comment. We would like to give you credit in both the draft and final reports for any corrective actions taken as a result of this memorandum. Therefore, we request that you keep us abreast (in electronic format) of all corrective actions you take or have taken to address the recommendations. You may e-mail me at

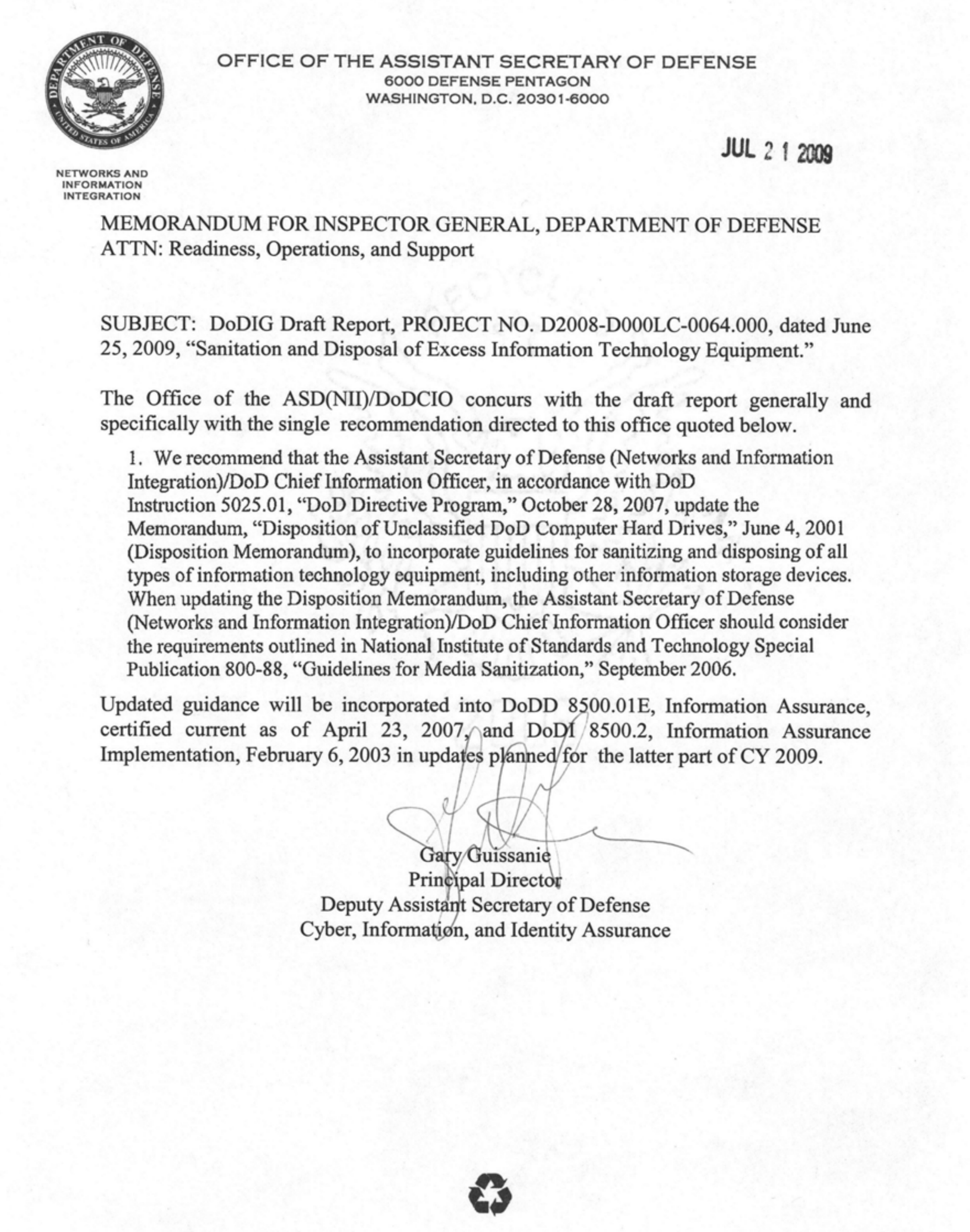
[redacted]

Rhonda L. Ragsdale

Rhonda L. Ragsdale
Acting Program Director
Readiness, Operations, and Support

cc: Department of the Navy Chief Information Officer
Naval Air Systems Command Office of Inspector General
Naval Facilities Command Office of Inspector General

Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer Comments



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NETWORKS AND
INFORMATION
INTEGRATION

JUL 2 1 2009

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Readiness, Operations, and Support

SUBJECT: DoDIG Draft Report, PROJECT NO. D2008-D000LC-0064.000, dated June 25, 2009, "Sanitation and Disposal of Excess Information Technology Equipment."

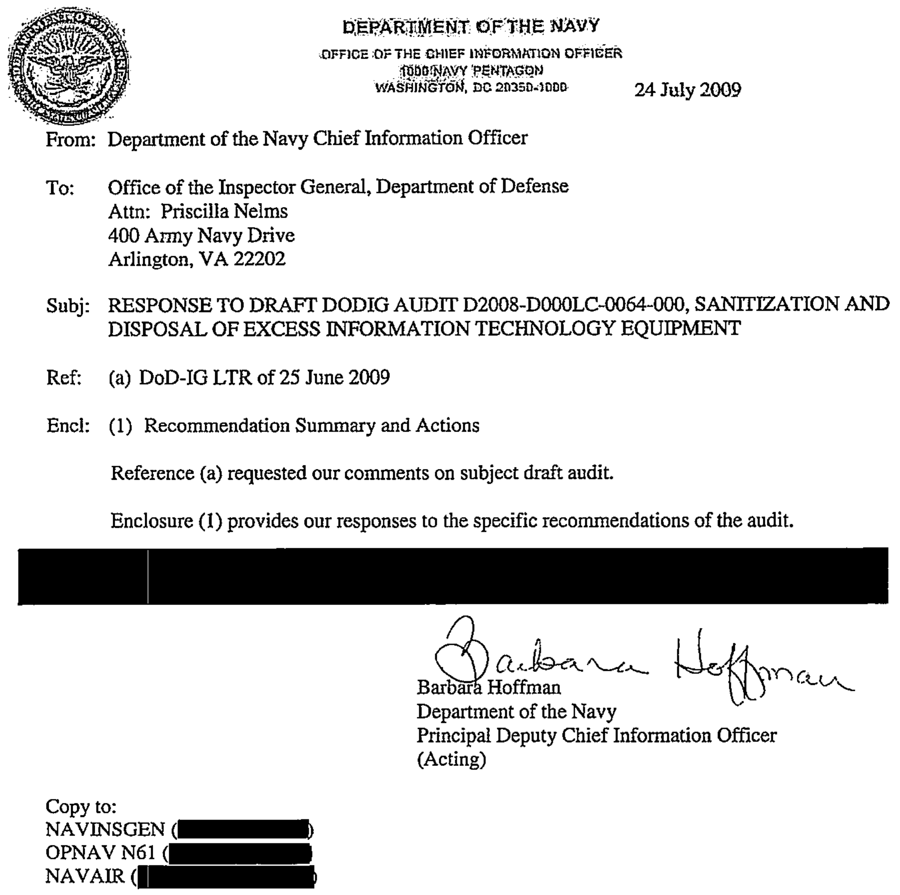
The Office of the ASD(NII)/DoDCIO concurs with the draft report generally and specifically with the single recommendation directed to this office quoted below.

> 1. We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, in accordance with DoD Instruction 5025.01, "DoD Directive Program," October 28, 2007, update the Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001 (Disposition Memorandum), to incorporate guidelines for sanitizing and disposing of all types of information technology equipment, including other information storage devices. When updating the Disposition Memorandum, the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer should consider the requirements outlined in National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," September 2006.

Updated guidance will be incorporated into DoDD 8500.01E, Information Assurance, certified current as of April 23, 2007, and DoDI 8500.2, Information Assurance Implementation, February 6, 2003 in updates planned for the latter part of CY 2009.

Gary Guissanie
Principal Director
Deputy Assistant Secretary of Defense
Cyber, Information, and Identity Assurance

Department of the Navy Chief Information Officer Comments



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

24 July 2009

From: Department of the Navy Chief Information Officer

To: Office of the Inspector General, Department of Defense
Attn: Priscilla Nelms
400 Army Navy Drive
Arlington, VA 22202

Subj: RESPONSE TO DRAFT DODIG AUDIT D2008-D000LC-0064-000, SANITIZATION AND DISPOSAL OF EXCESS INFORMATION TECHNOLOGY EQUIPMENT

Ref: (a) DoD-IG LTR of 25 June 2009

Encl: (1) Recommendation Summary and Actions

Reference (a) requested our comments on subject draft audit.

Enclosure (1) provides our responses to the specific recommendations of the audit.

[redacted]

Barbara Hoffman

Barbara Hoffman
Department of the Navy
Principal Deputy Chief Information Officer
(Acting)

Copy to:
NAVINSGEN ([redacted])
OPNAV N61 ([redacted])
NAVAIR ([redacted])

Enclosure (1) – DRAFT DODIG AUDIT D2008-D000LC-0064-000, SANITIZATION AND DISPOSAL OF EXCESS INFORMATION TECHNOLOGY EQUIPMENT - Recommendation Summary and Actions

The DON Chief Information Officer (CIO) concurs in all findings of the audit, and submits the following response to the recommendations addressed to the Navy including NAVAIR.

DoD-IG Recommendation #3: We recommend that the Department of the Navy Chief Information Officer establish and implement guidelines for sanitizing and disposing of all types of information technology equipment including other information storage devices in accordance with current and future sanitization and disposal policy issued by the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer. When establishing and implementing guidelines, the Department of the Navy Chief Information Officer should consider the requirements outlined in National Institute of Standards and Technology Special Publication 800-88, {Guidelines for Media Sanitization," September 2006.

DON CIO COMMENT: Concur

DON CIO will coordinate establishment of such policy within the Department, including the Navy, Marine Corps, and the Chief of Naval Operations Special Assistant for Security (N09N2). Estimated completion date for interim policy is 30 December 2009.

DoD-IG Recommendation #4: We recommend that the Deputy Chief of Naval Operations for Communications Networks update the Navy Information Assurance Publication 5239-26, "Remanence Security Guidebook", May 2000, to comply with the current version of the Disposition Memorandum, "Disposition of DoD Computer Hard Drives," June 4, 2001, and any updates coming out of Recommendation 1.

OPNAV N613 COMMENT: Concur.

Short-term: OPNAV N61 will continue working with DoN CIO on a coordinated DoN CIO, OPNAV N09N2, and OPNAV N6 message to address weaknesses identified by the audit. Estimated release of the DoN CIO message is 31 August 2009.

Mid-term: OPNAV N61 will coordinate publication of an updated Navy Information Assurance 5239-26. The update will address the Assistant Secretary of Defense (ASD) Memo "Disposition of unclassified DOD Computer Hard Drives June 4 2001, additional types of media, and consider the National Institute of Standards and Technology (NIST) 800-88 Guidelines for Media Sanitization, Sep 2006. Estimated completion of an updated Navy Information Assurance Publication 5239.26 is 29 January 2010.

DoD-IG Recommendation #6: We recommend that the Commander, Naval Air Warfare Center Aircraft Division (NAWCAD):

a. Require all personnel responsible for sanitization and disposal to comply with the Memorandum, "Disposition of Unclassified DoD computer hard Drives," June 4, 2001, and any future updates.

b. Account for all hard drives removed from their computer shells.

c. Account for hard drives removed from their computer shells that contain sensitive information in an electronic record-keeping system as required by DoD Instruction 5000.64, "Accountability and management of DoD Owned Equipment and Other Accountable Property," November 2, 2006.

d. Remove excess information technology equipment from the navy Enterprise Resource Planning (NERP) System only after obtaining an official receipt from the Defense Reutilization and Marketing Service processing center as required by DoD Instruction 5000.64, "Accountability and Management of DoD Owned Equipment and Other Accountable Property," November 2, 2006.

NAVAIR/NAWCAD Comment: Concur. NAWCAD will coordinate with the Naval Air Systems Command (NAVAIR) Chief Information Officer to develop appropriate processes and procedures relating to sanitization and disposal of excess IT equipment. The processes and procedures will address all requirements of Recommendation 6 and specify that only one system to generate disposal turn-in documents will be utilized. At this time, it is uncertain if the electronic Turn-In document (ETID) System will be utilized. Estimated date of completion is unknown at this time.

With regard to Recommendation 6.a, personnel responsible for the disposal of hard drives will be appropriately trained in accordance with Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001. Estimated date of completion is 30 November 2009.

With regard to recommendations 6.b. and 6.c., NAWCAD will evaluate the use of existing systems or develop/adopt a new system to capture all pertinent information in an electronic format accounting for all hard drives removed from their computer shells. NAWCAD will discontinue the use of National Security Agency for hard drive disposal and coordinate disposal with Defense Reutilization Marketing Service (DRMS) to handle future requirements. Estimate completion of this disposal process is 31 December 2009.

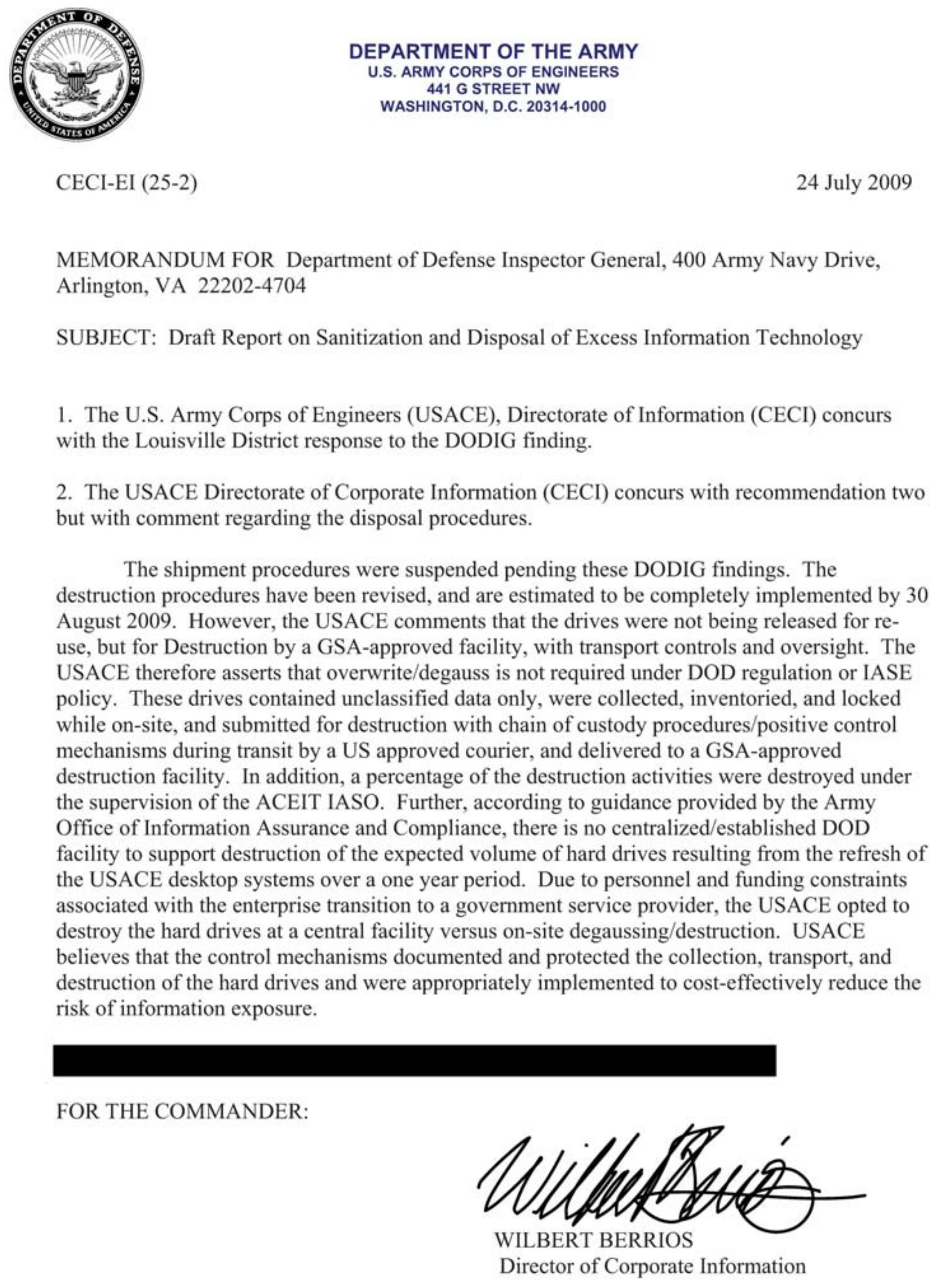
With regard to Recommendation 6.d., the NAWCAD Property Management Team will not remove equipment from the NERP System until receipt of completed documentation from the Naval Facilities Engineering Command (NAVFAC) Property Disposal Office. NAWCAD copies of the Requisition System Document (DD 1348) are stamped by the NAVFAC Property Disposal Office upon receipt of the equipment from the NAWCAD Property Management Team. Upon acceptance, the NAVFAC Property Disposal Office is responsible for the equipment and the NAWCAD Fixed Asset Team personnel annotate in the NERP system that the equipment has been disposed of. Please note that it takes years for additional documentation to be received from the DRMS Processing Centers. Action considered complete.

To date, listed below are NAWCAD's internal controls that have been instituted to implement the recommendation.

- A NAWCAD Excess Asset Form is signed by the fixed asset custodian at the time the IT equipment is picked up by the NAWCAD Property Management Team for the next step in the disposal process.
- The NAWCAD Excess Asset Form contains a statement which annotates, "All items containing fixed media must be cleared of all information prior to pick up or turn in. The person responsible for sanitizing the item must sign verifying that the fixed media contained in this item has been wiped clean/hard drive(s) removed in accordance with NAVSO Publication 5239.26."
- Once the DD 1348 is completed, the IT equipment is taken to the NAVFAC Property Disposal Office. Not all IT equipment is taken to the NAVFAC Property Disposal Office by the NAWCAD Property Management Team. Currently, some IT equipment is taken to the NAVDAC Property Disposal Office by data center or lab personnel. This IT equipment *is not* recorded in the NERP system.

- The NAWCAD Property Management Team does not remove equipment from the NERP System until receipt of completed documentation from the NAVFAC Property Disposal Office.
- The NAWCAD copies of the DD 1348s are stamped by the NAVFAC Property Disposal Office upon receipt of the equipment form the NAWCAD Property Management Team. Upon acceptance, the NAVFAC Property Disposal Office is responsible for the equipment and the NAWCAD Fixed Asset Team personnel annotate in the NERP system that the equipment has been disposed of.

U.S. Army Corps of Engineers Directorate of Corporate Information Comments



DEPARTMENT OF THE ARMY
U.S. ARMY CORPS OF ENGINEERS
441 G STREET NW
WASHINGTON, D.C. 20314-1000

CECI-EI (25-2)

24 July 2009

MEMORANDUM FOR Department of Defense Inspector General, 400 Army Navy Drive, Arlington, VA 22202-4704

SUBJECT: Draft Report on Sanitization and Disposal of Excess Information Technology

1. The U.S. Army Corps of Engineers (USACE), Directorate of Information (CECI) concurs with the Louisville District response to the DODIG finding.

2. The USACE Directorate of Corporate Information (CECI) concurs with recommendation two but with comment regarding the disposal procedures.

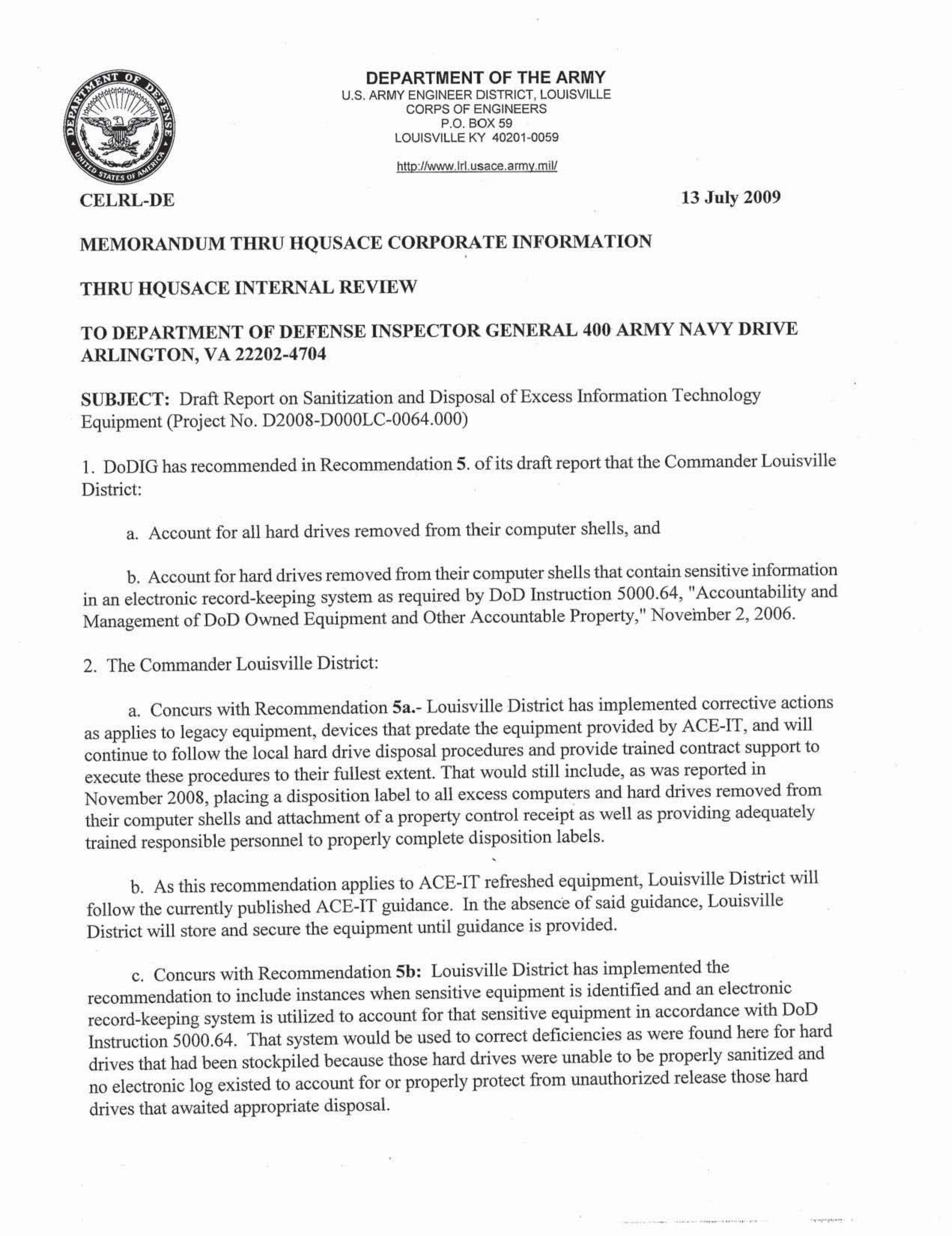
The shipment procedures were suspended pending these DODIG findings. The destruction procedures have been revised, and are estimated to be completely implemented by 30 August 2009. However, the USACE comments that the drives were not being released for re-use, but for Destruction by a GSA-approved facility, with transport controls and oversight. The USACE therefore asserts that overwrite/degauss is not required under DOD regulation or IASE policy. These drives contained unclassified data only, were collected, inventoried, and locked while on-site, and submitted for destruction with chain of custody procedures/positive control mechanisms during transit by a US approved courier, and delivered to a GSA-approved destruction facility. In addition, a percentage of the destruction activities were destroyed under the supervision of the ACEIT IASO. Further, according to guidance provided by the Army Office of Information Assurance and Compliance, there is no centralized/established DOD facility to support destruction of the expected volume of hard drives resulting from the refresh of the USACE desktop systems over a one year period. Due to personnel and funding constraints associated with the enterprise transition to a government service provider, the USACE opted to destroy the hard drives at a central facility versus on-site degaussing/destruction. USACE believes that the control mechanisms documented and protected the collection, transport, and destruction of the hard drives and were appropriately implemented to cost-effectively reduce the risk of information exposure.

[redacted]

FOR THE COMMANDER:

WILBERT BERRIOS
Director of Corporate Information

U.S. Army Corps of Engineers Louisville District Comments



DEPARTMENT OF THE ARMY
U.S. ARMY ENGINEER DISTRICT, LOUISVILLE
CORPS OF ENGINEERS
P.O. BOX 59
LOUISVILLE KY 40201-0059

http://www.lrl.usace.army.mil/

CELRL-DE 13 July 2009

MEMORANDUM THRU HQUSACE CORPORATE INFORMATION

THRU HQUSACE INTERNAL REVIEW

TO DEPARTMENT OF DEFENSE INSPECTOR GENERAL 400 ARMY NAVY DRIVE ARLINGTON, VA 22202-4704

SUBJECT: Draft Report on Sanitization and Disposal of Excess Information Technology Equipment (Project No. D2008-D000LC-0064.000)

1. DoDIG has recommended in Recommendation **5**. of its draft report that the Commander Louisville District:

a. Account for all hard drives removed from their computer shells, and

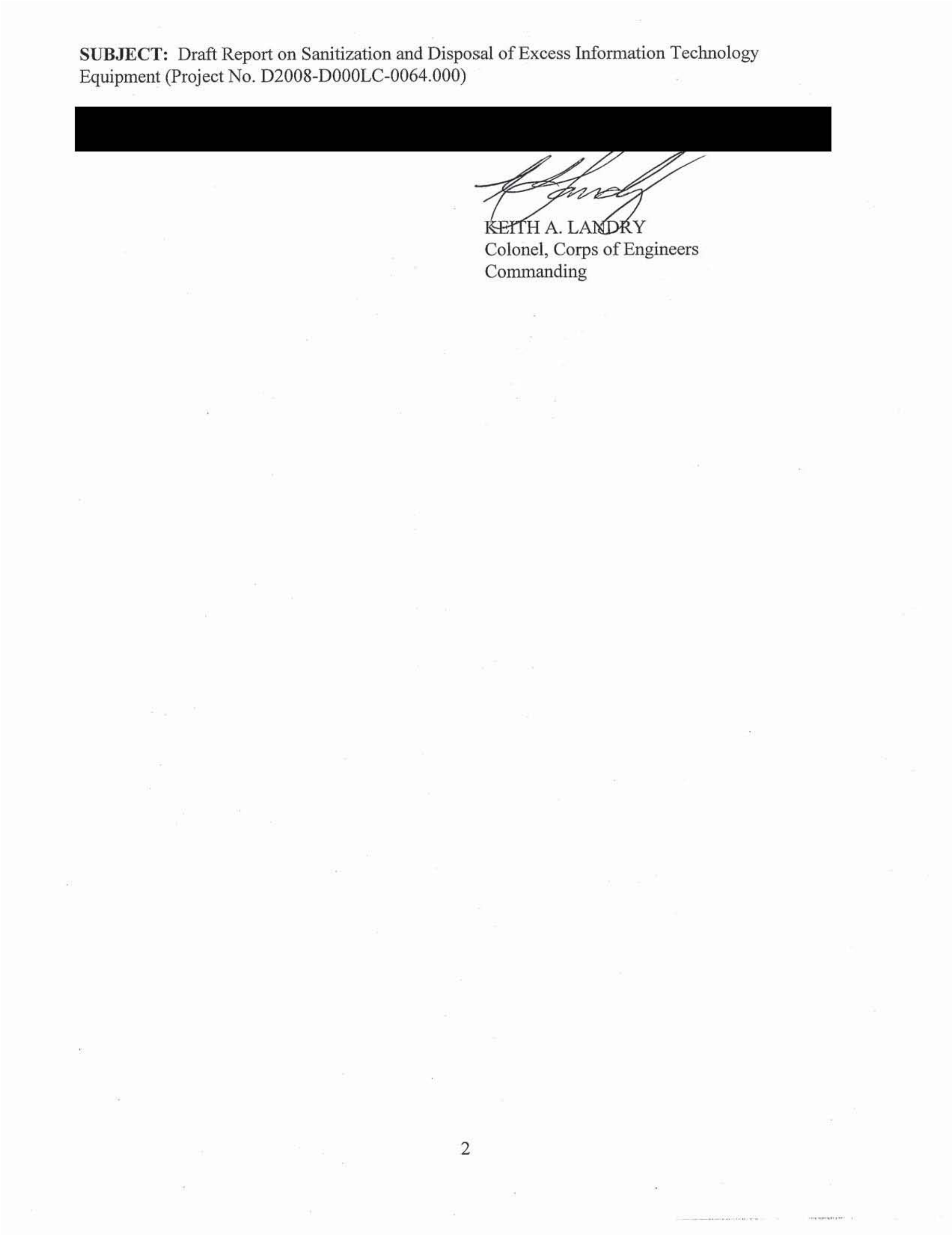
b. Account for hard drives removed from their computer shells that contain sensitive information in an electronic record-keeping system as required by DoD Instruction 5000.64, "Accountability and Management of DoD Owned Equipment and Other Accountable Property," November 2, 2006.

2. The Commander Louisville District:

a. Concurs with Recommendation **5a.**- Louisville District has implemented corrective actions as applies to legacy equipment, devices that predate the equipment provided by ACE-IT, and will continue to follow the local hard drive disposal procedures and provide trained contract support to execute these procedures to their fullest extent. That would still include, as was reported in November 2008, placing a disposition label to all excess computers and hard drives removed from their computer shells and attachment of a property control receipt as well as providing adequately trained responsible personnel to properly complete disposition labels.

b. As this recommendation applies to ACE-IT refreshed equipment, Louisville District will follow the currently published ACE-IT guidance. In the absence of said guidance, Louisville District will store and secure the equipment until guidance is provided.

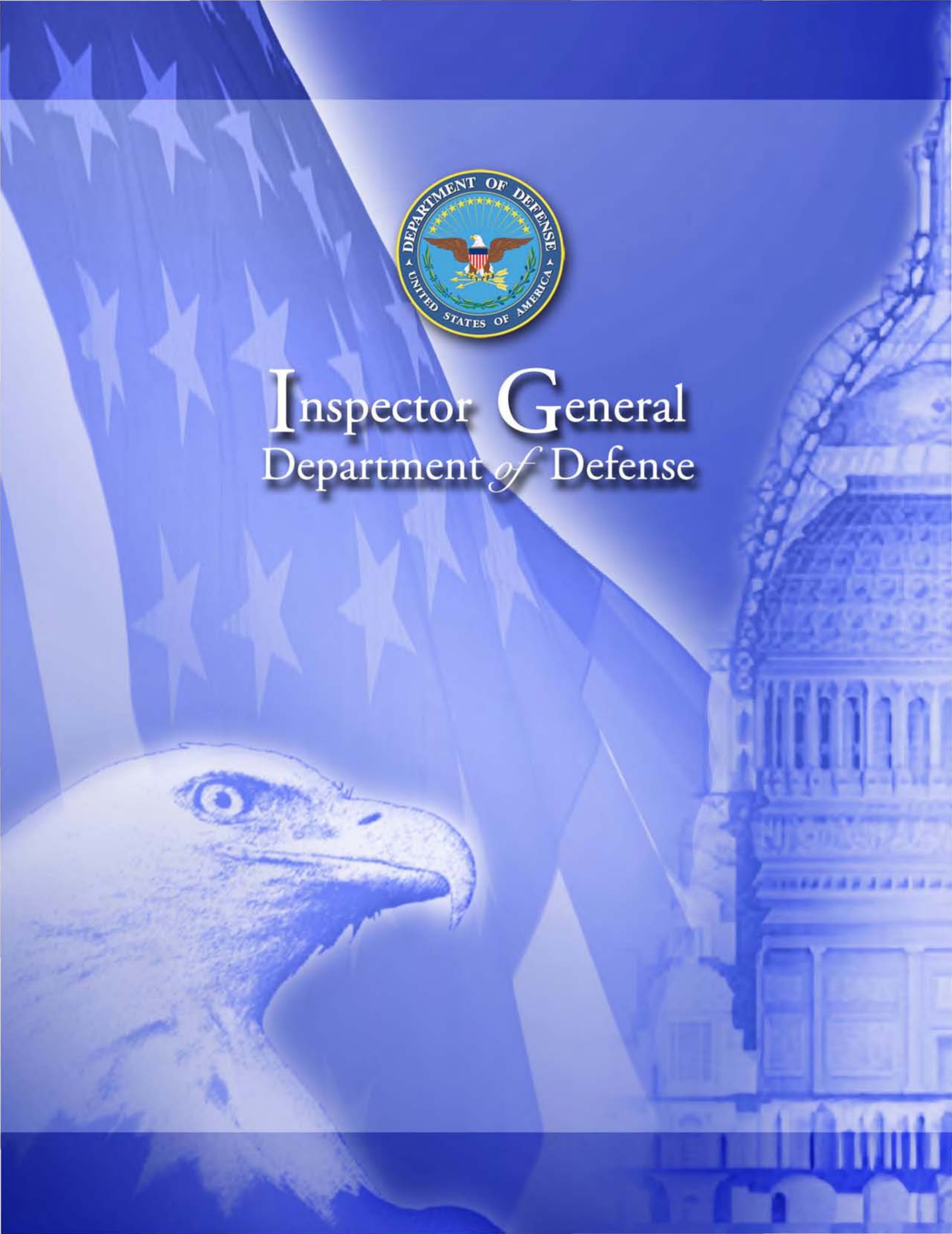
c. Concurs with Recommendation **5b:** Louisville District has implemented the recommendation to include instances when sensitive equipment is identified and an electronic record-keeping system is utilized to account for that sensitive equipment in accordance with DoD Instruction 5000.64. That system would be used to correct deficiencies as were found here for hard drives that had been stockpiled because those hard drives were unable to be properly sanitized and no electronic log existed to account for or properly protect from unauthorized release those hard drives that awaited appropriate disposal.



SUBJECT: Draft Report on Sanitization and Disposal of Excess Information Technology Equipment (Project No. D2008-D000LC-0064.000)

[redacted]

KEITH A. LANDRY
Colonel, Corps of Engineers
Commanding



Inspector General
Department of Defense